

ФГБОУ ВО «Уральский государственный юридический университет»

ТЕХНОЛОГИИ XXI ВЕКА В ЮРИСПРУДЕНЦИИ

**Материалы
Всероссийской научно-практической конференции
(Екатеринбург, 24 мая 2019 года)**

Екатеринбург
2019

УДК 34
ББК 67.3
Э14

Редакционная коллегия:

Д. В. Бахтеев, кандидат юридических наук, доцент кафедры криминалистики Уральского государственного юридического университета (отв. редактор)

А. А. Беляков, доктор юридических наук, профессор, заведующий кафедрой криминалистики Уральского государственного юридического университета

Э14 Технологии XXI века в юриспруденции: материалы Всероссийской научно-практической конференции (Екатеринбург, 24 мая 2019 года) / под ред. Д. В. Бахтеева. — Екатеринбург: Уральский государственный юридический университет. — 187 с.

ISBN 978-5-7845-0600-9

В сборнике представлены статьи учёных-юристов, представителей юридической практики и начинающих исследователей, принявших участие во Всероссийской научно-практической конференции «Технологии XXI века в юриспруденции», посвящённой отдельным проблемам юридических науки и практики, связанных с современными технологиями.

УДК 34
ББК 67.3

Материалы представлены в авторской редакции

Конференция была организована при финансовой поддержке Российского фонда фундаментальных исследований в рамках научного проекта 18-29-16001\18 «Комплексное исследование правовых, криминалистических и этических аспектов, связанных с разработкой и функционированием систем искусственного интеллекта».

ISBN 978-5-7845-0600-9

©Уральский государственный
юридический университет, 2019.

СОДЕРЖАНИЕ

Аmineва Зульфия Фарисовна	
ПРИМЕНЕНИЕ ТЕХНИЧЕСКИХ СРЕДСТВ ПРИ СОБИРАНИИ ДОКАЗАТЕЛЬСТВ ...6	
Антропов Алексей Владимирович	
АКТУАЛЬНЫЕ ПРОБЛЕМЫ ПРИМЕНЕНИЯ ЦИФРОВОЙ ФОТОГРАФИИ В ХОДЕ ПРОИЗВОДСТВА ТЕХНИКО-КРИМИНАЛИСТИЧЕСКИХ И ПОЧЕРКОВЕДЧЕСКИХ ЭКСПЕРТИЗ.....10	
Бахтеев Дмитрий Валерьевич	
ЭТИКО-ПРАВОВЫЕ МОДЕЛИ ИСПОЛЬЗОВАНИЯ СИСТЕМ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА16	
Беляков Александр Алексеевич, Бахтеев Дмитрий Валерьевич	
МОБИЛЬНЫЙ СПРАВОЧНИК СЛЕДОВАТЕЛЯ: СОДЕРЖАНИЕ И ТЕХНИЧЕСКИЕ УСЛОВИЯ РАЗРАБОТКИ.....23	
Брунцов Андрей Сергеевич	
ТЕХНОЛОГИЯ СОБИРАНИЯ, ИССЛЕДОВАНИЯ И ИСПОЛЬЗОВАНИЯ СМС И ПЕРЕПИСОК В МЕССЕНДЖЕРАХ И СОЦИАЛЬНЫХ СЕТЯХ КАК ДОКАЗАТЕЛЬСТВА В СУДЕБНОМ РАЗБИРАТЕЛЬСТВЕ27	
Галиханова Карина Ришатовна, Рачева Нелли Витальевна	
ИСПОЛЬЗОВАНИЕ БЕСПИЛОТНЫХ ЛЕТАТЕЛЬНЫХ АППАРАТОВ В ДЕЯТЕЛЬНОСТИ ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ.....31	
Дерюгин Роман Александрович, Жижилева Анастасия Александровна	
ПЕРСПЕКТИВЫ РАЗВИТИЯ ЦИФРОВОЙ КРИМИНАЛИСТИКИ В УСЛОВИЯХ ИНФОРМАЦИОННОГО ОБЩЕСТВА40	
Долинин Владимир Николаевич, Кабитова Юлия Равилевна, Елькина Полина Сергеевна	
ТЕХНОЛОГИИ СОБИРАНИЯ, ИССЛЕДОВАНИЯ И ИСПОЛЬЗОВАНИЯ ЭЛЕКТРОННО-ЦИФРОВЫХ ДОКАЗАТЕЛЬСТВ.....47	
Желватых Александр Александрович	
ОПАСНОСТИ КРИПТОВАЛЮТНЫХ «ПИРАМИД»: ОПЫТ СУДЕБНОЙ ПРАКТИКИ ...58	
Зимин Владимир Владимирович	
НАУЧНО-ТЕХНИЧЕСКИЕ ДОСТИЖЕНИЯ И ПРЕСТУПЛЕНИЯ БУДУЩЕГО: ВОПРОСЫ КРИМИНОЛОГИЧЕСКОГО ПРОГНОЗИРОВАНИЯ И УПРЕЖДАЮЩЕЙ КРИМИНАЛИЗАЦИИ61	
Коваленко Ксения Евгеньевна, Коваленко Наталья Евгеньевна, Кузьмина Анна Сергеевна	
ВВЕДЕНИЕ В ПРОГРАММУ ПОДГОТОВКИ ВОДИТЕЛЕЙ ЭЛЕКТРОННЫХ СИСТЕМ ОБУЧЕНИЯ*65	
Кодан Сергей Владимирович	

ИНФОРМАЦИОННЫЙ ПОДХОД В ЮРИДИЧЕСКОМ ИСТОЧНИКОВЕДЕНИИ	70
Колмыков Владимир Сергеевич	
ПРОБЛЕМЫ РЕАЛИЗАЦИИ ПРИНЦИПА ДОСТУПНОСТИ ЭЛЕКТРОННОГО ПРАВОСУДИЯ В ГРАЖДАНСКОМ ПРОЦЕССЕ	76
Костомаров Кирилл Валерьевич	
НЕКОТОРЫЕ ОСОБЕННОСТИ ФИКСАЦИИ ДОКАЗАТЕЛЬСТВ ПРИ РАССЛЕДОВАНИИ НЕЗАКОННОГО ДОСТУПА К КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ	81
Косьяненко Елена Михайловна	
ПЕРСПЕКТИВЫ ПРАВОВОГО РЕГУЛИРОВАНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА. ИНТЕЛЛЕКТУАЛЬНО-ПРАВОВОЙ АСПЕКТ	85
Кручинина Надежда Валентиновна	
ЭТИЧЕСКИЕ И ПРАВОВЫЕ ВОПРОСЫ ИСКУССТВЕННОЙ РЕПРОДУКЦИИ ЧЕЛОВЕКА	90
Кучин Иван Васильевич	
РЕГУЛИРОВАНИЕ КРИПТОВАЛЮТНЫХ ОБМЕННИКОВ	94
Мазунин Яков Маркиянович, Сидорова Ксения Сергеевна	
ОРГАНИЗАЦИОННЫЕ ОСОБЕННОСТИ ПРОИЗВОДСТВА ДОПРОСА С ИСПОЛЬЗОВАНИЕМ ВИДЕОКОНФЕРЕНЦ-СВЯЗИ.....	98
Никитина Елена Викторовна	
НЕКОТОРЫЕ ВОПРОСЫ СОБИРАНИЯ ЭЛЕКТРОННО-ЦИФРОВЫХ ДОКАЗАТЕЛЬСТВ.....	103
Олейникова Юлия Олеговна	
К ВОПРОСУ ОБ ИСПОЛЬЗОВАНИИ ГЕНОМНОЙ ИНФОРМАЦИИ ПРИ РАСКРЫТИИ ПРЕСТУПЛЕНИЙ	108
Пичугов Михаил Сергеевич	
ДЕАНОНИМИЗАЦИЯ ПРЕСТУПНИКА, СОВЕРШИВШЕГО ПРЕСТУПЛЕНИЕ В СЕТИ «ИНТЕРНЕТ»	113
Пучков Владислав Олегович	
ЭЛЕКТРОННЫЕ ДОКАЗАТЕЛЬСТВА В ГРАЖДАНСКОМ ПРОЦЕССУАЛЬНОМ ПРАВЕ США.....	118
Пушкарева Александра Игоревна, Сытикова Регина Игоревна	
ВОЗМОЖНОСТИ ИСПОЛЬЗОВАНИЯ УСЛУГ СУРРОГАТНОГО МАТЕРИНСТВА ДЛЯ ПАР, ПРИНАДЛЕЖАЩИХ К ЛГБТ-СООБЩЕСТВУ	121

Рачева Нелли Витальевна, Скорб Яна Владимировна	
СОВРЕМЕННЫЕ ТЕХНОЛОГИИ СОБИРАНИЯ И ИССЛЕДОВАНИЯ ЭЛЕКТРОННО-ЦИФРОВЫХ ДОКАЗАТЕЛЬСТВ ПРИ РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ, СВЯЗАННЫХ С НЕЗАКОННЫМ СБЫТОМ НАРКОТИЧЕСКИХ СРЕДСТВ, ПСИХОТРОПНЫХ ВЕЩЕСТВ И ИХ АНАЛОГОВ	125
Романов Алексей Николаевич, Руколеев Виталий Александрович	
ПРОБЛЕМНЫЕ ВОПРОСЫ МЕХАНИЗМА ВЗАИМОДЕЙСТВИЯ СУДА С ЛИЦАМИ, УЧАСТВУЮЩИМИ В СУДОПРОИЗВОДСТВЕ	135
Савоськин Александр Владимирович	
СТАНОВЛЕНИЕ В РОССИИ КОНСТИТУЦИОННОГО ПРАВА НА ОБРАЩЕНИЕ В СЕТИ ИНТЕРНЕТ	140
Семис-оол Индира Сергековна	
«ЗАСЛУЖИВАЮЩИЙ ДОВЕРИЯ» ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ	145
Смахтин Евгений Владимирович, Зеленкина Ольга Юрьевна	
ТРАНСФОРМАЦИЯ ЭЛЕКТРОННО-ЦИФРОВЫХ СЛЕДОВ В ЭЛЕКТРОННО-ЦИФРОВЫЕ ДОКАЗАТЕЛЬСТВА: ВОПРОСЫ ТЕОРИИ И ПРАКТИКИ	150
Сысуева Елена Николаевна	
ВНЕДРЕНИЕ ЭЛЕКТРОННОГО ДОКУМЕНТАОБОРОТА В ОРГАНЫ ПРОКУРАТУРЫ РФ	156
Холстинин Роберт Николаевич	
ЦИФРОВЫЕ СИСТЕМЫ В ЧЕЛОВЕЧЕСКОМ ИЗМЕРЕНИИ. ВОПРОСЫ РЕГУЛИРОВАНИЯ СЕТИ «ИНТЕРНЕТ».....	160
Чёрный Антон Васильевич	
ТЕХНОЛОГИИ ОХРАНЫ РЕЗУЛЬТАТОВ ИНТЕЛЛЕКТУАЛЬНОЙ ДЕЯТЕЛЬНОСТИ.....	166
Чуваткин Борис Юрьевич	
РЕЗУЛЬТАТ РАБОТЫ ИСКУССТВЕННОЙ НЕЙРОННОЙ СЕТИ КАК ОБЪЕКТ ИНТЕЛЛЕКТУАЛЬНЫХ ПРАВ	171
Щелконогова Елена Владимировна	
УГОЛОВНОЕ ПРАВО ON-LINE: ТЕОРИЯ И ПРАКТИКА ЦИФРОВИЗАЦИИ	177
Цахуев Альберт Вагабович	
СОБИРАНИЕ ЭЛЕКТРОННЫХ ДОКАЗАТЕЛЬСТВ ПРИ РАССЛЕДОВАНИИ УЧАСТИЯ ГРАЖДАН РОССИИ В НЕЗАКОННЫХ ВООРУЖЕННЫХ ФОРМИРОВАНИЯХ НА ТЕРРИТОРИИ ИНОСТРАННОГО ГОСУДАРСТВА	182

Аминева Зульфия Фарисовна

Соискатель кафедры уголовного процесса,
Уральский государственный юридический университет
(г. Екатеринбург)
basyrovaz@mail.ru

ПРИМЕНЕНИЕ ТЕХНИЧЕСКИХ СРЕДСТВ ПРИ СОБИРАНИИ ДОКАЗАТЕЛЬСТВ

Аннотация: Доказательства и доказывание – важные вопросы, которые определяют сущность и содержание уголовного процесса. Доказывание состоит в собирании, проверке и оценке доказательств в целях установления обстоятельств, предусмотренных ст. 73 УПК РФ. Представляется, что краткий анализ особенностей применения технических средств при собирании доказательств позволит определить их значимость для достижения задач уголовного судопроизводства.

Ключевые слова: Доказывание, собирание доказательств, электронный документ, технические средства, допустимость доказательств.

Собирание доказательств – начальная и необходимая стадия доказывания, содержание которой в уголовно-процессуальной литературе определяется по-разному. А. И. Винберг рассматривал собирание доказательств как «совокупность действий по обнаружению, фиксации, изъятию и сохранению различных доказательств»¹. П. А. Лупинская определяла собирание доказательств, как «совершение лицом, производящим дознание, следователем, прокурором, судом предусмотренных законом процессуальных действий, направленных на обнаружение, истребование, получение и закрепление в установленном порядке доказательств»². А. Д. Прошляков, В. С. Балакшин, Ю. В. Козубенко указывают, что «собирание доказательств – элемент уголовно-процессуального доказывания, представляющий собой уголовно-процессуальную деятельность уполномоченных на то органов, должностных лиц и участников процесса, осуществляемую способами и в порядке, предусмотренными законом по выявлению, отысканию, обнаружению, закреплению, изъятию и сохранению фактических данных и их источников с целью установления обстоятельств, имеющих значение для правильного разрешения уголовного дела»³. Нам импонирует указанное определение, так как в нем отражен круг субъектов доказывания, в который включены не только органы предварительного расследования, но и другие участники процесса. В этой связи, мы считаем обоснованным и справедливым мнение А. А. Давлетова, который указывает, что защитник также является субъектом доказывания по уголовным делам⁴.

По нашему мнению, собирание доказательств представляет собой деятельность уполномоченных органов и участников уголовного судопроизводства, которая осуществляется способами и в порядке, предусмотренными уголовно-процессуальным законом, и направлена на обнаружение, закрепление, изъятие и сохранение фактических данных и их источников с целью установления обстоятельств, имеющих значение для правильного разрешения уголовного дела.

¹ Винберг Л. И. Криминалистика. Раздел 1: Введение в науку. М., 1962. С. 16–17.

² Лупинская П. А. Доказательства и доказывание в новом уголовном процессе // Российская юстиция. 2002. № 7. С. 5–8.

³ Прошляков А. Д. Уголовный процесс: учебник / А. Д. Прошляков, В. С. Балакшин, Ю. В. Козубенко. М., 2016. С. 285.

⁴ Давлетов А. А. Правомочия защитника по собиранию доказательств в современной модели уголовного процесса России / А. Давлетов, Л. Юсупова. // Уголовное право. 2009. № 3. С. 77-80. Режим доступа: <https://elibrary.ru/item.asp?id=12903752> (дата обращения: 26.03.2019).

Этап обнаружения доказательств включает действия субъектов доказывания по отысканию, выявлению тех или иных фактических данных, которые могут приобрести доказательственное значение. На данной стадии собирания доказательств субъект доказывания имеет дело не с доказательством, а с фактическими данными, которые по его предположению еще только могут стать доказательствами, то есть с отпечатками события, еще не имеющими процессуального статуса доказательств. Как правило, указанные сведения добываются посредством оперативно-розыскной деятельности. Здесь могут применяться средства освещения, беспилотные летательные аппараты для осмотра мест происшествия на труднодоступных участках, оптические приборы. Необходимо отметить плюсы применения беспилотных летательных аппаратов – обеспечение получения и передачи на наземную станцию управления в режиме реального времени видео- и фотоизображения местности, координат наземных объектов по заданию оператора, а также сбор, накопление и комплексная обработка видеoinформации. Данные, полученные с помощью беспилотных летательных аппаратов, помогают в определении путей подхода к месту преступления, отхода от него, выявлению следов, в поиске пропавших без вести лиц.

Фиксация доказательств – следующий этап собирания доказательств, цель которого запечатлеть объект доказывания в определенных (процессуальных) формах. В процессуальной практике используются различные формы фиксации:

- 1) вербальная – протоколирование, звукозапись;
- 2) графическая – графическое изображение (схематические и масштабные планы, чертежи, рисунки);
- 3) предметная – изъятие самого предмета, изготовление материальных моделей (получение слепков);
- 4) наглядно-образная – фотографирование, киносъемка, видеосъемка.

В научной литературе нередко используются иные термины: отдельные процессуалисты пишут о «закреплении доказательств, об их «процессуальном оформлении», понимая под ними «отражение в процессуальных актах, обнаруженных следователем фактических данных»¹, «процессуальное удостоверение и документирование собранных доказательств»². В криминалистической литературе акцент делается на объектах фиксации, а также на средствах и методах фиксации³.

Так, С. А. Шейфер понимает под фиксацией доказательств систему следственных и процессуальных действий, направленных на преобразование воспринятой следователем «доказательственной информации, а также информации об источниках, условиях и способах ее получения, в форму, обеспечивающую эффективное (максимально полное) сохранение и использование полученных данных в процессе доказывания»⁴.

По нашему мнению, только после придания доказательственной информации, обнаруженной уполномоченным лицом или участниками судопроизводства, надлежащей процессуальной формы (формы показаний, заключений эксперта и т.д.), полученные сведения становятся доказательствами.

Однако не во всех странах на законодательном уровне закреплено обязательное протоколирование следственных и процессуальных действий. Так, В. А. Семенов отмечает, что сотрудники полиции США фиксируют результаты своей беседы (опроса) с участниками уголовного судопроизводства в своем блокноте, а впоследствии – в отчете по

¹ Белкин А. Р. Теория доказывания в уголовном судопроизводстве. М., 2005. С. 189.

² Агибалова В. С. Процессуальные и иные документы как источники доказательств в уголовном судопроизводстве: дис. ... канд. юрид. наук: 12.00.09. Краснодар, 2003. С. 33–58.

³ Беляков А. А. Криминалистическая техника. Практикум / А. А. Беляков, Л. Я. Драпкин, В. Н. Карагодин, В. В. Котов и др. Екатеринбург: Изд-во УрГЮА, 2000. С. 3–10. Режим доступа: <https://elibrary.ru/item.asp?id=12903752> (дата обращения: 26.03.2019).

⁴ Шейфер С. А. Собрание доказательств по уголовному делу: проблемы законодательства, теории и практики: монография. М, 2015. С. 12.

итогах расследования уголовного дела. УПК ФРГ предусматривает для ряда случаев не только протоколирование, но и обязательную аудио- или видеозапись хода следственного действия. Так, при допросе свидетеля производятся аудиозапись или видеосъемка, если показания дает лицо моложе 16 лет, если оно существенно пострадало в результате преступления, или существует опасение, что свидетель не сможет быть допрошен во время судебного разбирательства, и запись необходима для установления истины¹.

УПК РФ также предусматривает стенографирование, киносъемку, аудио- и видеозапись, но без соответствующего протокола юридической силы результаты применения технических средств не имеют.

В связи с этим В. А. Родивилина отмечает, что в современном мире целесообразно использовать электронно-цифровую форму документов, в том числе и в уголовном процессе². Необходимо отметить такие положительные характеристики электронного документа, как высокое качество фиксации, компактность, надежность, быстроту и удобство в использовании. Кроме того, нельзя не согласиться с мнением П. С. Пастухова, который отмечает, что письменный документ становится анахронизмом в информационном обществе, при повсеместном распространении электронных гаджетов и электронном документообороте³. Действительно, в современном обществе, где превалирующую роль в общественных отношениях играют информационные ресурсы, допустим электронный документооборот. Указанное в значительной степени позволит ускорить сроки предварительного расследования. Однако нельзя забывать, что доказательства, полученные с помощью технических средств, должны обладать в соответствии со ст. 88 УПК РФ свойствами достоверности и допустимости.

Изъятие доказательств – стадия собирания доказательств, которая обеспечивает возможность использования изъятых данных для доказывания, приобщения их к делу, а также служит средством их сохранения для следствия и суда. В тех случаях, когда речь идет о вещественных доказательствах, изъятие которых в натуре по каким-либо причинам нецелесообразно или невозможно, в качестве средств изъятия выступают некоторые формы и способы фиксации. Строго говоря, доказательство при этом не изымается, а изымаются, переносятся, переходят на новый объект его доказательственные свойства. Новый объект, носитель этих свойств, является производным вещественным доказательством.

Сохранение доказательств заключается в принятии мер по сохранности самих доказательств либо их доказательственных свойств, а также обеспечивает возможность их использования следователем или судом. Меры по сохранению доказательств могут носить процессуальный характер (например, хранение доказательств среди материалов дела), но могут быть и технико-криминалистическими (консервация объектов, имеющих доказательственное значение, покрытие их защитными пленками и т.п.).

Результаты проведенного нами анализа позволяют сделать некоторые частные выводы, представляющие интерес для нашего исследования. Технические средства применяются на всех этапах собирания доказательств, но объем их использования зависит от конкретных целей того или иного этапа. Представляется важным отметить анахронизм в условиях информационного общества письменного документооборота, который, на наш взгляд, целесообразно дополнить электронным. Вместе с тем, учитывая специфику уголовного судопроизводства, необходимо закрепить правило о том, что электронный документ может иметь доказательственную силу, только если известно его происхождение, и он аутентичен.

¹ Семенцов В. А. Избранные статьи по уголовному процессу. Краснодар: Просвещение-Юг, 2013. С. 16.

² Родивилина В. А. Процессуальные особенности использования технических средств в стадии предварительного расследования: дис. ... канд. юрид. наук: 12.00.09. Иркутск, 2016. С. 75.

³ Пастухов П. С. К вопросу о создании процедуры использования «электронных доказательств» в уголовном судопроизводстве // Международное уголовное право и международная юстиция. 2015. № 2. С. 5-8.

Это позволит участникам уголовного судопроизводства представлять суду свои электронные документы, равно как и иные материалы, имеющие доказательственное значение, и требовать признания их доказательствами.

Список литературы

1. Агибалова В. С. Процессуальные и иные документы как источники доказательств в уголовном судопроизводстве: дис. ... канд. юрид. наук: 12.00.09. Краснодар, 2003. 230 с.
2. Белкин А. Р. Теория доказывания в уголовном судопроизводстве. М., 2005. 528 с.
3. Беляков А. А. Криминалистическая техника. Практикум / А. А. Беляков, Л. Я. Драпкин, В. Н. Карагодин, В. В. Котов и др. Екатеринбург: Изд-во УрГЮА, 2000. 124 с. Режим доступа: <https://elibrary.ru/item.asp?id=12903752>.
4. Винберг Л. И. Криминалистика. Раздел 1: Введение в науку. М., 1962. 96 с.
5. Давлетов А. А. Правомочия защитника по собиранию доказательств в современной модели уголовного процесса России / А. Давлетов, Л. Юсупова. // Уголовное право. 2009. № 3. С. 77-80. Режим доступа: <https://elibrary.ru/item.asp?id=12903752>.
6. Лупинская П. А. Доказательства и доказывание в новом уголовном процессе // Российская юстиция. 2002. № 7. С. 5-8.
7. Пастухов П. С. К вопросу о создании процедуры использования «электронных доказательств» в уголовном судопроизводстве // Международное уголовное право и международная юстиция. 2015. № 2. С. 5-8.
8. Прошляков А. Д. Уголовный процесс: учебник / А. Д. Прошляков, В. С. Балакшин, Ю. В. Козубенко. М., 2016. 874 с.
9. Родивилина В. А. Процессуальные особенности использования технических средств в стадии предварительного расследования: дис. ... канд. юрид. наук: 12.00.09. Иркутск, 2016. 218 с.
10. Семенцов В. А. Избранные статьи по уголовному процессу. Краснодар: Просвещение-Юг, 2013. 593 с.
11. Шейфер С. А. Собираение доказательств по уголовному делу: проблемы законодательства, теории и практики: монография. М, 2015. 112 с.

Zulfiya F. Amineva

Competitor of the Department of Criminal Procedure Law
Ural State Law University
(Russia, Yekaterinburg)
basyrovaz@mail.ru

USE OF TECHNICAL MEANS AT COLLECTION OF EVIDENCE

Abstract: Evidence and substantial showing are important question defining entity of the Criminal Code (CC). Substantial showing consists collecting «checking and evaluating the evidences with the aim to settle the surcumstanses specified in the article 73 of CC of Russian Federation. It is expected that brief analyses of technical means peculiarities at the stage of evidence collection allows emphasize their importance for meeting the goals of criminal justice system.

Keywords: proof, collection of evidence, electronic document, technical means, admissibility of evidence.

Антропов Алексей Владимирович
Заведующий криминалистической лабораторией
Уральский государственный юридический университет
(г. Екатеринбург)
aa-64@mail.ru

АКТУАЛЬНЫЕ ПРОБЛЕМЫ ПРИМЕНЕНИЯ ЦИФРОВОЙ ФОТОГРАФИИ В ХОДЕ ПРОИЗВОДСТВА ТЕХНИКО-КРИМИНАЛИСТИЧЕСКИХ И ПОЧЕРКОВЕДЧЕСКИХ ЭКСПЕРТИЗ*

Аннотация: В статье рассматриваются проблемы, возникающие при использовании цифровых средств фиксации и исследования в ходе судебно-почерковедческих, и технико-криминалистических экспертиз и пути решения организационно-правовых и технических вопросы, связанные с использованием, оформлением и оценкой результатов применения судебной фотографии.

Ключевые слова: экспертиза, цифровая фотография, почерк, судебное почерковедение, судебно-почерковедческая экспертиза, технико-криминалистическая экспертиза документов.

Судебная экспертная деятельность базируется на следующих принципах, зафиксированных в статье № 4 Федерального закона № 73-ФЗ «О государственной судебно-экспертной деятельности в Российской Федерации» от 31.05.2001 года: законность, соблюдение прав и свобод человека и гражданина, права юридического лица, независимость, объективность, всесторонность, полнота проведенного исследования.

Соблюдение указанных принципов напрямую связано с целью и задачами судебно-исследовательской фотографии, которая призвана фиксировать и исследовать данные, обнаруженные в ходе экспертизы. Точная, объективная и полная фиксация этих данных диктуется интересами установления истины по делу. Фотоснимки, изготовленные с соблюдением правил, успешно используются в целях решения как диагностических, так и идентификационных задач. При этом фотосъемка не влияет на сохранность и состояние снимаемого объекта.

Благодаря различным приёмам и способам судебной фотографии удастся продемонстрировать не только сравнительное исследование совпадающих признаков, что является важным удостоверительным фактом в экспертизе, но и показать доказательственную значимость установленных фактических данных.

Судебно-исследовательская фотография представляет собой систему научных положений, средств, приемов, методов и способов фотосъемки, используемых для фиксации и исследования объектов в ходе экспертизы. Она призвана дать в распоряжение экспертов фотографические средства и методы анализа свойств криминалистических объектов, а также обеспечить наглядную фиксацию их общего вида, состояния и иллюстрацию хода и результатов проведенных исследований.

С фотографией как методом получения изображения связаны такие важные для эксперта признаки как: наглядность, сравнительная точность, универсальность отражения, большая чувствительность, высокая разрешающая способность и оперативность. Современные цифровые технологии внедряются во все сферы человеческой деятельности, облегчая труд, экономя время и средства. Но не следует слепо внедрять новые технологии

* Исследование выполнено при финансовой поддержке Российского фонда фундаментальных исследований в рамках научного проекта 18-29-16001\18 «Комплексное исследование правовых, криминалистических и этических аспектов, связанных с разработкой и функционированием систем искусственного интеллекта».

в процесс производства судебных экспертиз. Использование неапробированных и необоснованных приёмов, методов и способов исследований часто негативно сказывается на результатах исследовательской деятельности. Цифровая технология в судебной фотографии стала неотъемлемым элементом как судебно-запечатлевающей, так и исследовательской фотографии.

Однако с ее внедрением возник ряд проблем организационно-правового и технического характера (практического).

Только на первый взгляд проблемы организационно-правового характера находят разрешение в уголовно-процессуальном законодательстве (ст. 9; п. 6 ст. 164; п. 8 ст. 166 УПК РФ). При глубоком анализе данных норм обнаруживается, что регулирование идет только в самых общих чертах и даже не предполагает отсылочных или бланкетных норм по данному вопросу. Более подробную регламентацию можно обнаружить в иных федеральных законах и подзаконных нормативно-правовых актах (ФЗ «О государственной судебно-экспертной деятельности в РФ»; Информационное письмо ГУ ЭКЦ МВД России № 37/11-1676 от 24.04.2003г.; приказ от 29 июня 2005г. № 511 «Вопросы организации производства судебных экспертиз в экспертно-криминалистических подразделениях органов внутренних дел Российской Федерации»). Основным правовым пробелом регулирования применения цифровой фотографии в уголовном судопроизводстве является процессуальное оформление. Методы, разработанные для пленочных фотографий в связи с отличием фото процессов, не могут быть применены, а порядок приобщения фотографий, регулируемый информационным письмом ГУ ЭКЦ МВД России № 37/11-1676 от 24.04.2003 г., устарел применительно к настоящему уровню развития науки и техники.

На практике к заключению эксперта прилагается только фототаблица с иллюстрацией общего вида исследуемых объектов и изображениями сравнительного исследования, а наличие цифрового оригинала фотоснимков даже не упоминается. Достоверность информации, содержащейся в копиях, может вызвать сомнения, так как при копировании или обработке изображений с ними могут произойти существенные изменения. Следовательно, возникает необходимость разработки способа сохранения и приобщения к материалам дела оригиналов цифровых фотоснимков.

С внедрением цифровых технологий появилась проблема, связанная с фальсификацией изображений (в отношении пленочных фотографий она практически отсутствовала). Путем производства несложных действий можно удалить с цифрового изображения какой-либо объект либо его часть.

В связи с наличием данных возможностей необходимо и целесообразно обязать эксперта передавать цифровые изображения на материальном носителе вместе с заключением и в последующем хранить при материалах уголовного дела.

При изготовлении фотоснимков эксперту периодически приходится прибегать к обработке фотографий с целью улучшения изображения при помощи фоторедакторов на персональном компьютере. Данный вопрос частично регламентирован законом, однако все установленные требования (описание устройства ввода, используемый фотоаппарат, объектив, освещение, характеристики исходного файла с изображением, графический редактор, процедуры обработки изображений с указанием параметров и степени изменения яркости, контраста, цветового баланса и т. д.) являются ничтожными при отсутствии в материалах уголовного дела цифрового оригинала подвергшихся редактированию снимков. Также одного только описания действий по редактированию крайне недостаточно, более надежной гарантией является создание специальной базы, хранящей оригиналы цифровых фотоснимков и информацию обо всех пошаговых изменениях в них.

Заключение эксперта – процессуальный документ, в котором излагаются результаты проведенного исследования. Эксперт составляет письменное заключение от своего имени, удостоверяет его своей подписью и личной печатью и направляет в орган, назначивший экспертизу. Закон определяет основные элементы содержания заключения эксперта, не

устанавливая его структуры. В судебно-экспертной практике такая структура выработана и нашла отражение в ведомственных нормативных правовых актах.

Методика исследования описывается таким образом, чтобы можно было судить о полноте применения её экспертом и, при необходимости, проверить правильность выводов путем воспроизведения исследования.

Каждому вопросу должен соответствовать, как правило, определенный раздел исследовательской части. Исследовательская часть акта экспертизы в целях наглядности сопровождается иллюстративными материалами – фотоснимками, схемами, чертежами и т. д., содержащимися в приложении.

Многие объекты, фигурирующие в следственной фотографии, методы, приёмы используются также и в исследовательской фотографии. Однако среди них имеются и специфические, свойственные только исследовательской фотографии методы и приёмы.

К заключению, как правило, прилагаются следующие иллюстрации:

1) снимки упаковки и общего (первоначального) вида объектов исследования, имеющие особое значение при последующем изменении этих объектов;

2) снимки отдельных фрагментов объектов с иллюстрацией и указанием выявленных признаков;

3) контрольные снимки к ним, так как обводка и условные обозначения затрудняют восприятие выявленных деталей.

Каждый снимок должен сопровождаться ссылкой на него в тексте, подробными пояснительными записями. Иллюстрации удостоверяются подписями эксперта и печатью органа судебной экспертизы.

К заключению должны быть приложены оставшиеся после исследования объекты, в том числе образцы, а также фототаблицы, схемы, графики, таблицы и другие материалы, подтверждающие выводы эксперта.

Для того, чтобы заключение эксперта могло быть проверено при его оценке с позиций обоснованности и достоверности сделанных выводов лицом или органом, назначившим экспертизу, и быть убедительным для других участников процесса, его выводы анализируются. В основу такой оценки должна быть положена: *во-первых*, проверка соответствия формы и содержания заключения; *во-вторых*, проверка наличия в заключении описания всех действий, совершение которых обязательно при производстве экспертиз; *в-третьих*, формально-логический анализ исследовательской и выводной части заключения с целью установления правильности логической формы выводов эксперта, аргументации и отсутствия противоречий. Этот процесс облегчается при наличии в заключении надлежаще оформленных и выполненных иллюстрационных материалов.

Каждая исследовательская фотография проходит три стадии. Сначала она создается при помощи необходимой аппаратуры. В это время могут задействоваться те или иные методы и способы исследования фотографии либо самого объекта. Затем снимок оформляется как часть заключения эксперта или приложения к нему. Третьей стадией является ее анализ лицом или органом, назначившим экспертизу. При этом данное лицо должно иметь доступ к информации на всех стадиях создания фотоснимка. Только после этого можно анализировать информацию о признаках и свойствах объекта, которая была обнаружена и зафиксирована в фотографии.

Однако введение цифровых технологий позволяет наглядно продемонстрировать некоторые свойства объекта. Так, при исследовании вариационности подписного материала в рамках производства почерковедческой экспертизы были совмещены путем наложения преобразованные в различные цвета сравнительные образцы подписи. Именно данная иллюстрация позволяет каждому участнику уголовного судопроизводства убедиться в наличии признаков вариационности.



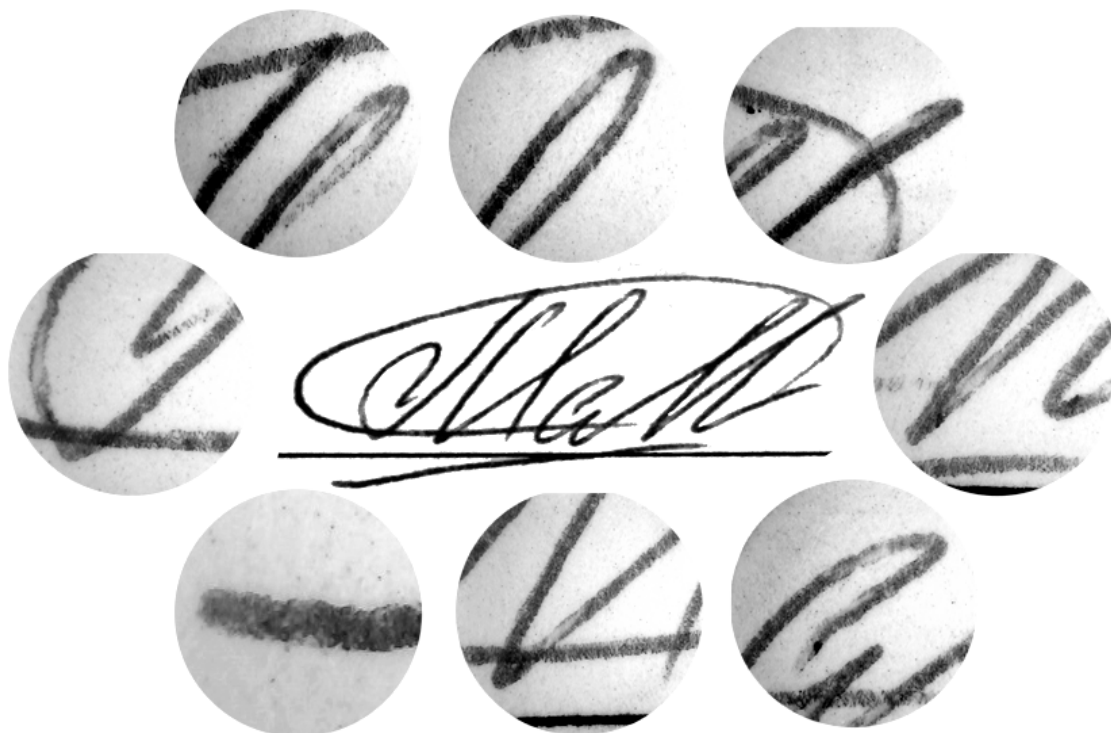
Необходимо отметить, что иллюстрирование должно производиться по общим правилам криминалистики – от общего к частному. Нарушение данного правила может привести к тому, что представленная иллюстрация будет вырвана из контекста, и при помощи нее будут подтверждаться необоснованные, неверные выводы. Так, при производстве первичной экспертизы эксперт сделал вывод о том, что имеет место техническое исполнение подписи путем передавливания штрихов с последующей обводкой, обосновав это наличием признаков необычности выполнения отдельных элементов, а также полным сопоставлением конфигурации вдавленных штрихов и подписи. Данный факт эксперт подтвердил следующей иллюстрацией.



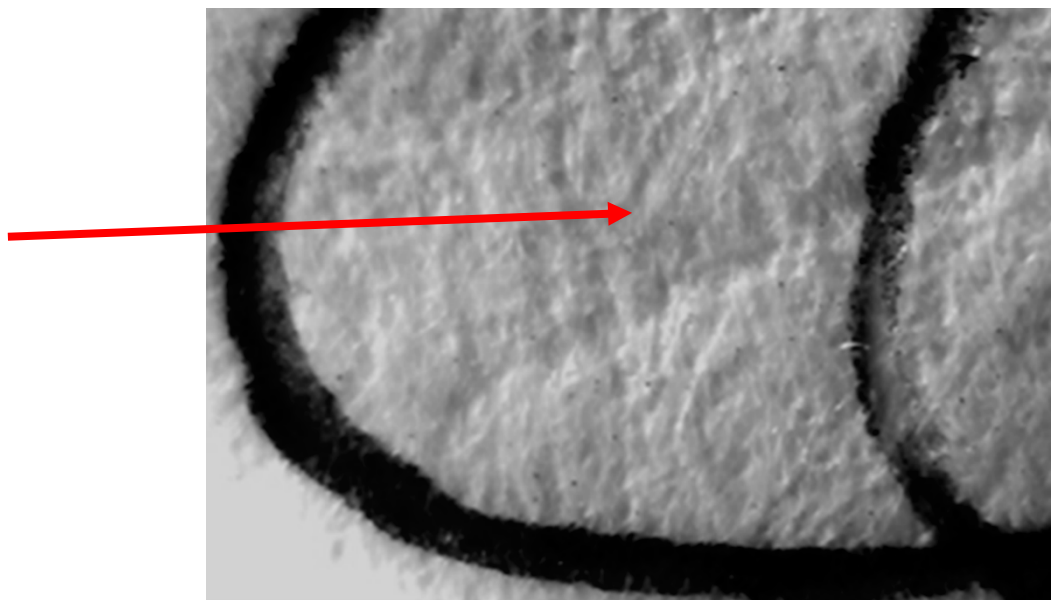
Однако при производстве повторной экспертизы был произведен снимок общего вида исследуемого объекта



На данном снимке видно, что конфигурация вдавленных штрихов не совпадает с подписью. Более того, при производстве макросъемки в косопадающем свете было обнаружено, что необычность выполнения отдельных элементов связана с пересечением в данных местах с вдавленными штрихами.



Выявленные элементы позволяют убедиться в отсутствии признаков технического исполнения подписи.



Наличие правильно выполненных иллюстраций позволяет каждому участнику уголовного судопроизводства понять логический ход производства экспертизы и убедиться в правильности и обоснованности выводов эксперта.

Это далеко не полный перечень всех проблем, возникающих при использовании цифровых средств фиксации и исследования. Для преодоления данных недостатков необходимо решить организационно-правовые и технические вопросы, связанные с использованием, оформлением и оценкой результатов применения судебной фотографии.

Alexey V. Antropov
Head of Forensic Laboratory
Ural State Law University
(Russia, Ekaterinburg)
aa-64@mail.ru

CURRENT PROBLEMS OF DIGITAL PHOTOGRAPHY APPLICATION IN THE COURSE OF MANUFACTURING TECHNICAL CRIMINALISTIC AND HANDWRITING EXAMINATIONS

Abstract: The article discusses the problems arising from the use of digital means of fixation and research in the course of forensic handwriting, and technical examinations of documents and ways of solving organizational, legal and technical issues related to the use, design and evaluation of the results of applying forensic photography.

Keywords: examination, digital photography, handwriting, forensic handwriting examination, technical examination of documents.

Бахтеев Дмитрий Валерьевич

Кандидат юридических наук, доцент кафедры криминалистики

Уральский государственный юридический университет

(г. Екатеринбург)

dmitry.bakhteev@gmail.com

ЭТИКО-ПРАВОВЫЕ МОДЕЛИ ИСПОЛЬЗОВАНИЯ СИСТЕМ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА*

Аннотация: В статье описаны модели использования систем искусственного интеллекта при возникновении ответственности за ущерб, возможности наделения систем искусственного интеллекта правами. Физический ущерб может быть вызван ошибками в распознавании объектов или базовыми «этическими настройками» программного обеспечения. Это создает ситуацию неопределённой ответственности. Ответственность за такие ошибки может быть возложена либо на разработку программного обеспечения, либо на пользователя, но только в том случае, если последний активно влиял на настройки системы. ИИ рассматривается как возможный субъект права на основе возможных подходов к искусственному интеллекту: как инструмент или партнер. Чтобы решить эту проблему, необходимо получить ответы на вопросы об осознании ИИ реальности и способности испытывать эмоции.

Ключевые слова: искусственный интеллект, искусственная нейронная сеть, этика искусственного интеллекта, мораль искусственного интеллекта, моделирование ИИ, принятие решений.

Увеличение вычислительной мощности компьютерных устройств привело к появлению систем искусственного интеллекта – программных или аппаратных комплексов, способных принимать автономные решения без участия человека как оператора. В феврале 2017 года Европарламент рассмотрел возможность правового регулирования статуса электронной личности для сложных роботов, способных принимать самостоятельные решения. В первую очередь это касалось беспилотного автотранспорта, однако в отдельных сферах человеческой деятельности отдельные проявления искусственного интеллекта уже активно используются или начинают внедряться, к примеру, банковская сфера, военные технологии, рекламная, страховая деятельность и т. д.

Подобного рода изменения влекут за собой трансформацию человеческого сознания, отношения людей к новым технологиям, их влиянию на жизнь отдельного человека и общества в целом. Это ставит перед наукой задачу определения возможных проблем этического характера, морально-этических и правовых основ системы «человек – искусственный интеллект». К настоящему времени круг вопросов, относящихся к данной тематике, сводится к следующим:

- обновлённые формальные основы индивидуальной и коллективной этики;
- возможности качественно-количественной оценки этического поведения;
- механизмы этического выбора и критерии принятия решений;
- взаимодействие человека и интеллектуальных компьютерных систем;
- взаимодействие общества и интеллектуальных компьютерных систем;

* Исследование выполнено при финансовой поддержке Российского фонда фундаментальных исследований в рамках научного проекта 18-29-16001\18 «Комплексное исследование правовых, криминалистических и этических аспектов, связанных с разработкой и функционированием систем искусственного интеллекта».

- нормативно-правовое регулирование функционирования систем искусственного интеллекта.

Большинство современных систем искусственного интеллекта (далее – ИИ) обладают реально или предполагаемо антропоморфизмом. Речь в данном случае не идёт о человекоподобных роботах; сходство с человеком в данном случае следует понимать функционально, то есть большинство задач, решаемых такими системами, сводятся к ускорению и уточнению того, что уже может совершать человек. Более того, в основе таких систем лежат субъективные представления их создателей, а архитектура искусственных нейронных сетей – наиболее доступной технологии искусственного интеллекта – воспроизводит принципы работы мозга человека. Исследования Баррета и Кейла в продемонстрировали, что при моделировании ситуации со всемогущим ИИ испытуемые наделяют его человекоподобными качествами^{1 2}.

До 20-го века единственным предсказуемым субъектом в системе жизнедеятельности человека был только человек. Однако сейчас уже можно говорить о появлении условных субъектов, которые способны оказывать вполне заметное влияние на общество и индивидов, которые человеком не являются, хотя и созданы им. Программное обеспечение способно привлекать человеческое внимание и инициировать определённые действия человека. Это может привести как к положительным изменениям в обществе, так и, при неправильном использовании, к негативным. Поведение человека в обществе ограничивается различными регуляторами: правом, морально-этическими, религиозными, корпоративными нормами, обычаями. Различия между предписаниями указанных нормативных систем обуславливают значительное число социальных противоречий и конфликтов, поэтому минимизация таких различий можно назвать одной из задач развития и совершенствования права.

Ключевым отличием систем искусственного интеллекта от более традиционных программных комплексов является их обучаемость. Возможности по обработке данных всегда зависят от опыта, который система ИИ набирает на стадии тренировки, обучаясь выявлять отдельные признаки и закономерности в предоставляемом для обучения массиве данных.

При этом, как и в случае с обучением и подготовкой человека-специалиста, обучение ИИ никогда не способно охватить все возможные сценарии и варианты его будущего функционирования. Соответственно, ИИ, подобно человеку, способен ошибаться. Любые ошибки способны причинить вред, однако наибольший вред ошибки ИИ способны причинить в физическом мире. Наиболее очевидными примерами ситуаций, в которых уже сейчас ощущается присутствие ИИ в физическом мире, являются автономные транспортные и боевые системы.

Основной риск, который заключается в функционировании таких объектов заключается в отсутствии полной прозрачности в основах их деятельности. Разработчикам программного обеспечения в силу конкуренции невыгодно раскрывать алгоритмы обучения и принятия решений коммерческих продуктов. Один из первых таких случаев произошёл в 2015 году при запуске беспилотных автомобилей под управлением ИИ, созданного компанией Nvidia.

Группы негативных ситуаций, возникающих с использованием ИИ в автономных мобильных системах, сводятся к следующим:

1. Риск совершения ошибки при распознавании объектов. К примеру, автономное транспортное средство может не распознать велосипедиста или пешехода в камуфляжной

¹ Barrett J. L., C. Keil F. C. Conceptualizing a Nonnatural Entity: Anthropomorphism in God Concepts // Cognitive psychology. 1996. Vol. 31. Issue 3. P. 219-247. DOI: 31. 219-47. DOI: 10.1006/cogp.1996.0017.

² Yudkowsky E. Artificial Intelligence as a Positive and Negative Factor in Global Risk // Global Catastrophic Risks / ed. N. Bostrom, M. M. Ćirković. 2008.

одежде (ложно-отрицательная ошибка), либо принять небольшую яму на дороге за значительное препятствие (ложно-положительная ошибка).

2. Базовые «этические настройки» программного обеспечения. В целом они сводятся к известной этической проблеме вагонетки и включают расстановку приоритетов при аварийной дорожной ситуации. К примеру, каким образом должен действовать ИИ, управляющий грузовиком,двигающимся на большой скорости, на дороге перед которым внезапно появляется группа людей, а на встречной полосе движется плотный поток автомобилей?

В последнем случае этические модели могут принимать следующие формы:

1. Совершить наезд на людей или выехать на встречную полосу, спровоцировав лобовое столкновение. Эти варианты предусматривают значительный риск гибели людей и причинения большого материального ущерба третьим лицам;

2. Съехать в кювет, что неминуемо вызовет критические повреждения автомобиля и угрозу жизни и здоровью водителя.

Такое ограниченное количество вариантов, которые могут обрабатываться с позиций человеческой этики вызвано ограничением познавательных способностей человека¹. «Экспериментальные данные указывают на то, что реализация этического поведения робота должна требовать лишь небольшого числа поведенческих альтернатив, которые должны быть сгенерированы и оценены. Оценка ограниченного числа поведенческих альтернатив улучшит отзывчивость роботов»².

Таким образом, поведение ИИ в аварийных ситуациях может иметь этическую окраску: быть альтруистичным или эгоистичным. Представляется, что в большинстве случаев настройки этичности будут производиться при тренировке ИИ, однако следует упомянуть интересную идею, согласно которой этическая ответственность может быть переложена на лицо, владеющее автономным автомобилем. Для этого потребуется программный или программно-аппаратный комплекс – т. н. «этическая кнопка», которая «переключала бы настройки автомобиля с «полностью альтруистичного» режима на «полностью эгоистичный» и обратно, при этом режим по умолчанию был бы беспристрастным³.

Иначе обстоит дело с автономными боевыми системами, к которым с определённой долей условности можно отнести военные, полицейские роботы и системы обеспечения домашней безопасности. Случаи наблюдения или разведки не вызывают крупных этических вопросов, однако прецеденты причинения интеллектуальными автономными физическими системами повреждений требуют анализа. Автономный боевой дрон, самостоятельно принимающий решение о поражении целей создаёт двойственную ситуацию: с одной стороны, ответственность за причинение смерти или повреждений должна быть возложена на сторону, которая применила данное устройство. С другой стороны, ни один индивидуальный человек не может нести ответственность за итоговое решение, то есть, дрон выступает в определённом смысле субъектом права. Также следует упомянуть проблему идентификации комбатантов и гражданских лиц в ходе боевых действий: если идентификация представителей своей стороны боевым роботом обеспечивается довольно просто (с помощью униформы или радиометок), то вопрос различения противников и гражданских лиц остаётся открытым. «Существует бесконечное число ситуаций, в которых применение оружия будет неуместным.

¹ Donoso M., Collins A., Koechlin E. Human cognition. Foundations of human reasoning in the prefrontal cortex // Science. 2014. Vol. 344. Issue 6191. P. 1481-1486. DOI: 344. 10.1126/science.1252254.

² Vanderelst D., Winfield A. An architecture for ethical robots inspired by the simulation theory of cognition // Cognitive Systems Research. 2018. Vol. 48. DOI: 10.1016/j.cogsys.2017.04.002.

³ Contissa G., Lagioia F., Sartor G. The Ethical Knob: ethically-customisable automated vehicles and the law // Artificial Intelligence Law. 2017. Vol. 25. Issue 3. P. 365-378. DOI: 10.1007/s10506-017-9211-z.

Достаточно подумать о детях, которых заставляют переносить разряженное оружие или комбатантов, которые занимаются похоронами своих погибших товарищей»¹.

С усложнением систем искусственного интеллекта возрастает количество вопросов относительно их возможности воспринимать, чувствовать и осознанно действовать. Люди уже продемонстрировали способность испытывать симпатию и эмпатию к роботам, будь это персонажи художественных произведений, домашние помощники или детские развивающие игрушки. В этом смысле системы искусственного интеллекта (как правило, овеществлённые) уже воспринимаются с точки зрения этики, применимой к домашним питомцам. Примером могут служить отключение серверов, обслуживающих роботов Jibo, которое многие пользователи восприняли как смерть своего компаньона и отреагировали крайне эмоционально². Но может ли искусственный интеллект стать хотя бы приблизительно равным человеку?

Для формирования представления о возможности наделения систем искусственного интеллекта субъектностью, человечество должно ответить на несколько частных вопросов:

- Способен ли ИИ осознавать реальность? В когнитивных науках отсутствует точное определение сознания, так что можем ли мы категорически утверждать, что машина не способна мыслить? Ранее считалось, что ключевым отличием человека от машины является возможность творчества, но современные искусственные нейронные сети уже продемонстрировали способность создавать художественные произведения: от живописи до стихов.

- Может ли ИИ испытывать негативные или позитивные эмоции? Принуждение свободного человека к выполнению неприятной для него работы с помощью силы мы считаем насилием и всячески осуждаем. Не считать ли в таком случае ситуацию, когда разработанную и натренированную для выполнения определённой задачи систему искусственного интеллекта перепрограммируют для выполнения совершенно других операций также проявлением насилия? Или перепрограммированная система уже считается совершенно другой и потому страдать не может? Или всё же такие системы несмотря на свою сложность и возможности являются не более, чем инструментом?

Такие вопросы могут показаться абсурдными, однако если мы не дадим на них категоричного и всеобщего ответа, вряд ли общество и государство смогут оказаться готовыми к развитию рассматриваемой технологии.

Дэвид Гункель предлагает четыре исчерпывающие модели позиционирования искусственного интеллекта относительно возможности признания их личностью и наделения их правами:

1. Роботы не могут иметь права, роботы не должны иметь права;
2. Роботы могут иметь права, роботы должны иметь права;
3. Роботы могут иметь права, но не должны иметь права;
4. Роботы не могут иметь права, но должны иметь права³.

Согласно первой модели, системы искусственного интеллекта или их физические воплощения (роботы) представляют из себя не более, чем инструмент. Инструмент – продукт деятельности человека и способ изготовления других предметов, в том числе и инструментов. Однако данная точка зрения имеет ряд существенных недостатков. Если инструмент призван облегчить труд человека, то ИИ может заменить своей деятельностью труд человека. При этом некорректным будет сравнение искусственного интеллекта со станками времён промышленной революции. Такие станки лишили работы множество людей, однако при этом они создали новые рабочие места. В случае автоматизации

¹ Lin P., Abney K., Bekey G. A. Robot Ethics: the Ethical and Social Implications of Robotics. Cambridge, Mass.: MIT Press, 2014. P. 118.

² Heater B. The lonely death of Jibo, the social robot. Режим доступа: <https://techcrunch.com/2019/03/04/the-lonely-death-of-jibo-the-social-robot/> (дата обращения: 17.05.2019).

³ Gunkel D. J. Robot rights. Cambridge, MA: MIT Press, 2018. 256 pp.

вообще и использования систем искусственного интеллекта в частности мы уже наблюдаем ликвидацию определённых профессий, в первую очередь – связанных с посредническими услугами: консультантов, диспетчеров, маркетологов и т. д. Можно возразить, что при этом увеличивается количество разработчиков искусственного интеллекта, однако увеличение числа программистов не идёт в сравнение с уменьшением рабочих мест других профессий.

Вторая модель предполагает создание «сильного» ИИ, по своим когнитивным возможностям сравнимым со способностями человека. При этом предполагается определённое равенство между человеком и системой искусственного интеллекта.

Данная проблема находится в области этики, однако должна рассматриваться и с правовых позиций. Если в будущем роботы и другие формы искусственного интеллекта обретут самосознание и будут способны испытывать эмоции, концепцию правосубъектности придётся на них распространить. Уже известны примеры, когда отдельными правами человека наделялись искусственные личности. К примеру, достаточно известный робот София с октября 2017 года является подданной Саудовской Аравии, а Shibuya Miri ИИ, программа, не имеющая физического воплощения, имитирующая речь и реакции 7-летнего мальчика, была признана гражданином Токио. До этого между 2004 и 2012 годами как минимум девять роботов были наделены специальным видом на жительство в Японии¹. Очевидно, что эти примеры носят скорее рекламный, популистский характер, однако являются первым прецедентом подобного рода. К настоящему времени до создания полноценного искусственного интеллекта, подобного человеческому, ещё далеко, однако исключать такой вариант нельзя, поэтому требуется разработка подходов к восприятию систем искусственного интеллекта как личностей и правового регулирования их статуса.

Если роботы достигнут определённого уровня когнитивных способностей, то есть, если они будут обладать очевидной моральной значимостью, такой как разум или чувствительность, тогда они, вероятно, будут претендовать на признание их морального статуса и должны иметь права, то есть некоторую долю привилегий, претензий, полномочий или иммунитетов². Очевидно, что для описания данной модели используется слишком много слов «если» и «вероятно». Это выражает степень неуверенности в возможности развития ИИ до таких пределов, однако исключать такую возможность всё же нельзя.

Третий сценарий предполагает по сути ситуацию рабства: человечество, формально признавая когнитивные способности систем искусственного интеллекта, по разным причинам предпочитает придерживаться инструментальной концепции и не признаёт личностных качеств ИИ. Учитывая множество социальных, национальных и расовых противоречий и предрассудков, к сожалению, такой вариант может оказаться вполне реальным.

Последний, четвёртый вариант, по сути, представляет максимально человеческое отношение человека к системе искусственного интеллекта. Описанные ранее случаи, фактически, являются примером реализации именно этой модели. Такое отношение может оказаться довольно опасным: «Социальные роботы, которые устанавливают с людьми эмоциональный контакт и, как следствие, последние глубоко доверяют роботам, что в свою очередь может быть использовано для манипулирования людьми ранее невозможными способами. Например, компания может использовать уникальные отношения робота со своим владельцем, чтобы робот убедил владельца приобрести продукты, которые компания хочет продвигать. Обратите внимание, что в отличие от человеческих отношений, где при нормальных обстоятельствах социальные

¹ Robertson J.. Human rights vs. Robot rights: Forecasts from Japan // *Critical Asian Studies*. 2014. Vol. 46. Issue 4. P. 571-598. DOI: 10.1080/14672715.2014.960707.

² Gunkel D. J. *Robot rights*. Cambridge, MA: MIT Press, 2018. 256 pp.

эмоциональные механизмы, такие как эмпатия и вина, предотвратят эскалацию таких сценариев»¹.

Подводя итог, отметим, что ИИ является крайне мощной технологией, напрямую или опосредованно влияющей на большинство сфер человеческой жизни, поэтому крайне важным является разработка и изучение этических основ функционирования таких систем. Понимание возможных рисков позволит обеспечить готовность общества и государства к развитию и распространению ИИ. Однако гармоничное и безрисковое развитие этой технологии возможно лишь при соблюдении ряда условий, таких как:

- прозрачность получения данных и методов их обработки. Недопустимо требовать от разработчиков ИИ принудительного опубликования программного кода, однако источники базы для тренировки сети и возможные настройки весов при обучении, если конечный продукт может, как было описано ранее, вызывать вопросы относительно своих действий, должны быть открыты. Кроме того, современные системы искусственного интеллекта, созданные на архитектурах искусственных нейронных сетей, содержат скрытый слой, на котором происходит недоступная человеку обработка данных. Возможно, в будущем появятся более открытые для понимания модели ИИ.

- Разработка правовых основ создания, внедрения и использования систем искусственного интеллекта в значимых областях жизнедеятельности: медицине, образовании, обеспечении правопорядка и т. д.

- Изучение этических основ использования систем искусственного интеллекта; разработка соответствующего кодекса этики.

- Разъяснительная работа с обществом: люди должны понимать значение систем искусственного интеллекта, доверять им, однако быть предупреждёнными о возможных рисках и опасностях использования этих систем.

Список литературы

1. Barrett J. L., C. Keil F. C. Conceptualizing a Nonnatural Entity: Anthropomorphism in God Concepts // *Cognitive psychology*. 1996. Vol. 31. Issue 3. P. 219-247. DOI: 10.1006/cogp.1996.0017.
2. Contissa G., Lagioia F., Sartor G. The Ethical Knob: ethically-customisable automated vehicles and the law // *Artificial Intelligence Law*. 2017. Vol. 25. Issue 3. P. 365-378. DOI: 10.1007/s10506-017-9211-z.
3. Donoso M., Collins A., Koechlin E. Human cognition. Foundations of human reasoning in the prefrontal cortex // *Science*. 2014. Vol. 344. Issue 6191. P. 1481-1486. DOI: 10.1126/science.1252254.
4. Gunkel D. J. Robot rights. Cambridge, MA: MIT Press, 2018. 256 pp.
5. Heater B. The lonely death of Jibo, the social robot. Режим доступа: <https://techcrunch.com/2019/03/04/the-lonely-death-of-jibo-the-social-robot/>.
6. Lin P., Abney K., Bekey G. A. Robot Ethics: the Ethical and Social Implications of Robotics. Cambridge, Mass.: MIT Press, 2014.
7. Robertson J. Human rights vs. Robot rights: Forecasts from Japan // *Critical Asian Studies*. 2014. Vol. 46. Issue 4. P. 571-598. DOI: 10.1080/14672715.2014.960707.
8. Vanderelst D., Winfield A. An architecture for ethical robots inspired by the simulation theory of cognition // *Cognitive Systems Research*. 2018. Vol. 48. DOI: 10.1016/j.cogsys.2017.04.002.
9. Yudkowsky E. Artificial Intelligence as a Positive and Negative Factor in Global Risk // *Global Catastrophic Risks* / ed. N. Bostrom, M. M. Ćirković. 2008. P. 308-345.

¹ Scheutz M. The Inherent Dangers of Unidirectional Emotional Bonds between Humans and Social Robots // Workshop on Roboethics at ICRA. 2009.

Dmitry V. Bakhteev
PhD in Law, Associate Professor of the Department of Criminalistics
Ural State Law University
(Russia, Yekaterinburg)
dmitry.bakhteev@gmail.com

ETHICAL AND LEGAL MODELS OF USING SYSTEMS OF ARTIFICIAL INTELLIGENCE

Abstract: The article describes models of using artificial intelligence systems in the occurrence of liability for damage, the possibility of endowing artificial intelligence systems with rights. Physical damage may be caused by errors in the recognition of objects, or by basic «ethical settings» of software. This creates a situation of uncertain responsibility. Responsibility for such errors can be assigned either to software development or to the user, but only if the latter has actively influenced the system settings. AI is considered as possible subject of law based on possible approaches to artificial intelligence: as a tool or a partner. To resolve this problem, it is necessary to receive answers to questions about AI's awareness of reality and the ability to experience emotions.

Keywords: artificial intelligence, artificial neural network, ethics ai, moral ai, modelling ai, decisionmaking.

Беляков Александр Алексеевич

Доктор юридических наук, профессор, заведующий кафедрой криминалистики
Уральский государственный юридический университет
(г. Екатеринбург)
aleks-1@inbox.ru

Бахтеев Дмитрий Валерьевич

Кандидат юридических наук, доцент кафедры криминалистики
Уральский государственный юридический университет
(г. Екатеринбург)
dmitry.bakhteev@gmail.com

**МОБИЛЬНЫЙ СПРАВОЧНИК СЛЕДОВАТЕЛЯ: СОДЕРЖАНИЕ И
ТЕХНИЧЕСКИЕ УСЛОВИЯ РАЗРАБОТКИ***

Аннотация: В работе рассматриваются форма и содержание мобильного справочника как инструмента как способа информационного обеспечения следственной деятельности. Приводятся технические требования к таким приложениям, типовая структура.

Ключевые слова: Crimlib.info, справочник следователя, мобильный справочник, информатизация.

Объём информации криминалистического, технического, физиологического характера в силу развития науки и техники значительно превышает ёмкость оперативной памяти следователя, особенно в ситуациях недостатка опыта или пробелов в образовании. С такой проблемой с разной степенью интенсивности сталкивались в любой исторический период существования следственной деятельности и практика выработала два относительно эффективных подхода к её решению: в худшем случае – методом проб и ошибок (что нельзя назвать оптимальным подходом к достижению задач уголовного судопроизводства), в лучшем – повышением (и актуализацией) квалификации следователя. Последнее может достигаться без отрыва следователя от служебной деятельности путём наставничества либо предоставления ему доступа к справочной литературе. О доступе к справочной информации и пойдёт речь в настоящей работе.

Доступ к справочной информации может быть реализован в двух вариантах: стационарном или мобильном. В первом случае воспользоваться таким источником следователь может либо в кабинетных условиях, либо в полевых, однако с определёнными неудобствами. В классическом виде справочники следователя представляют собой многостраничные труды, в книжном воплощении обладающие значительным физическим весом¹. Разумеется, в современную эпоху следователь может воспользоваться таким материалом в оцифрованном виде, однако тексты и иллюстрации, воспринимаемые с бумаги и с экрана должны обладать разными подходами к форматированию и оформлению. Современный человек, в том числе и следователь, в большинстве случаев всегда имеет с собой смартфон, умеет им пользоваться, более того, по мнению некоторых

* Исследование выполнено при финансовой поддержке Российского фонда фундаментальных исследований в рамках научного проекта 18-29-16001\18 «Комплексное исследование правовых, криминалистических и этических аспектов, связанных с разработкой и функционированием систем искусственного интеллекта».

¹ К примеру, Настольная книга следователя / под общ. ред. Г. Н. Сафонова. М.: Государственное издательство юридической литературы, 1949. 880 с.; Руководство для следователей / под общ. ред. В. В. Мозякова. М.: Издательство «Экзамен», 2005. 912 с.; Справочник следователя. Осмотр места происшествия / под ред. И. А. Попова. М.: ЦОКР МВД России, 2010. 302 с.

авторов смартфон уже представляет собой внешний орган человеческого организма, без которого полноценное функционирование затрудняется¹. Не погружаясь в дискуссию о перспективах этого аспекта современной жизни, укажем, что мобильные устройства позволяют, в числе прочего оптимизировать процессы доступа следователя к справочной информации, что неизбежно повлечёт за собой улучшение качества раскрытия и расследования преступлений. А. И. Бастрыкин отмечает, что «особую актуальность приобретает необходимость сочетания в работе следователей-криминалистов как практики и наработанного опыта расследования преступлений, так и новых знаний, сочетая их с использованием возможностей современной техники»².

Справочная информация может быть воплощена в форме мобильного приложения, однако её содержание и форма неизбежно будут иметь отличия от «классических» справочников и настольных книг следователя. Силами сотрудников кафедры криминалистики Уральского государственного юридического университета в настоящее время разрабатывается мобильное приложение «CrimLib.info – Справочник следователя». К основным характеристикам данного проекта (равно как и любого другого мобильного справочника) относятся:

1. Структура справочной информации. В отечественной, равно как и зарубежной криминалистике к настоящему времени сформировались несколько подходов к организации структуры справочной информации. Первая модель представлена в учебной литературе и предполагает изложение материала от общего к частному, от методологических основ науки и основополагающих концепций (теории идентификации, механизма слеодообразования и др.) к индивидуальным особенностям расследования отдельных видов и категорий преступлений. Вторая модель, как правило, реализована в справочниках, создаваемых для практических сотрудников. Их структура, в свою очередь, также может быть условно классифицирована на приоритетную и хронологическую. Приоритетная модель предполагает изложение информации от наиболее важной к наименее. Важность при этом, как правило, определяется наибольшими трудностями, с которыми сталкивается следователь. Хронологическая модель воспроизводит последовательность действий при расследовании преступлений: от проверочных мероприятий до составления обвинительного заключения (акта). Представляется, что мобильный справочник должен составлять по приоритетной модели. С нашей точки зрения, наибольшие трудности для следователя (особенно начинающего свой профессиональный путь) составляет производство осмотра места происшествия, допросов в сложных следственных ситуациях, планирование расследования, соответственно, основное внимание в мобильном приложении «CrimLib.info – Справочник следователя» будет уделяться именно указанным операциям.

2. Стилистические особенности подачи информации. В отличие от традиционных справочников, в мобильном справочнике нельзя допускать развернутых текстов, осложнённых вводными конструкциями, средствами художественной выразительности и т. п. Текст должен быть сжатым, а конкретный вопрос (к примеру, правила описания боеприпасов) должен раскрываться по возможности без использования дискуссионной терминологии, а его объём не должен превышать нескольких экранных страниц (в целях сокращения времени на поиск нужных сведений).

¹ Leave my iPhone alone: why our smartphones are extensions of ourselves // theguardian.com [Электронный ресурс]. Режим доступа: <https://www.theguardian.com/technology/2016/feb/19/iphone-apple-privacy-smartphones-extension-of-ourselves> (дата обращения: 17.05.2019).

² Бастрыкин А. И. О роли следователя-криминалиста в раскрытии и расследовании преступлений // Криминалистика – прошлое, настоящее, будущее: достижения и перспективы развития: материалы Международной научно-практической конференции, приуроченной к 60-летию образования службы криминалистики (Москва, 16 октября 2014 года). М.: Академия Следственного комитета Российской Федерации, 2014. – С. 4.

3. Формат подачи информации. Текст, читаемый с экрана мобильного устройства, должен быть выровнен не по ширине (как это принято в книгах), а по левому краю. Выбранный шрифт должен позволять читать текст на высокой скорости¹, быть контрастным по отношению к фону. Также должна быть предусмотрена возможность изменения регистра (размера шрифта). Учитывая, что следователю приходится работать в условиях плохого освещения, в том числе в ночное время, в мобильном справочнике должна присутствовать возможность переключения режима отображения текста в «ночной» (светлые буквы на тёмном фоне).

4. Безопасность использования. Современная криминалистика является открытой научно-практической дисциплиной, однако излишнее распространение справочной информации криминалистического характера явно нежелательно. Соответственно, в мобильном справочнике должны быть соблюдены стандарты безопасности, в том числе запрет копирования как данных самого приложения, так и данных пользователя.

С точки зрения приоритетности справочной информации для начинающего следователя были определены следующие основные разделы мобильного справочника:

1. Действия при следственном осмотре (с основным фокусом на осмотре места происшествия в различных ситуациях расследования);

2. Справочник по описанию объектов. Имеющие иллюстрации и схемы по описанию объектов недостаточно подходят для их восприятия с экрана небольшого мобильного устройства, поэтому в рамках рассматриваемого проекта осуществляет отрисовка новых иллюстраций.

3. Программы допросов. В данном разделе мобильного справочника содержатся типовые программы допросов, включающие в себя последовательность постановки вопросов, обстоятельства, подлежащие выяснению при допросе, в том числе промежуточные доказательственные факты, краткое описание основных тактических приёмов допроса подозреваемых, обвиняемых, потерпевших и свидетелей.

4. Судебные экспертизы. В данном разделе описывается порядок отбор образцов для сравнительного исследования, их упаковки и направления на экспертное исследование, приводятся перечни типовых вопросов по основным направлениям экспертных исследований.

5. Программы расследований: алгоритмы и планы расследований по отдельным видам и категориям преступлений для типовых следственных ситуаций;

6. Образцы процессуальных документов: примеры оформлений протоколов и постановлений.

Разработка и внедрение описанного приложения – не первый и не последний шаг в цифровизации деятельности правоохранительных органов. В перспективе внедрение технологий оперативного получения точной и актуальной информации должны привести к значительному повышению эффективности деятельности по раскрытию и расследованию преступлений.

Список литературы

1. Leave my iPhone alone: why our smartphones are extensions of ourselves // theguardian.com [Электронный ресурс]. Режим доступа: <https://www.theguardian.com/technology/2016/feb/19/iphone-apple-privacy-smartphones-extension-of-ourselves>.

2. Screws J. Quantitative Analysis of Font Type's Effect on Reading Comprehension. 2016. Режим доступа: <http://andrewd.ces.clemson.edu/courses/cpsc412/fall16/teams/reports/group7.pdf>.

¹ Screws J. Quantitative Analysis of Font Type's Effect on Reading Comprehension. 2016. Режим доступа: <http://andrewd.ces.clemson.edu/courses/cpsc412/fall16/teams/reports/group7.pdf> (дата обращения: 17.05.2019).

3. Бастрыкин А. И. О роли следователя-криминалиста в раскрытии и расследовании преступлений / Криминалистика – прошлое, настоящее, будущее: достижения и перспективы развития: материалы Международной научно-практической конференции, приуроченной к 60-летию образования службы криминалистики (Москва, 16 октября 2014 года). М.: Академия Следственного комитета Российской Федерации, 2014.
4. Настольная книга следователя / под общ. ред. Г. Н. Сафонова. М.: Государственное издательство юридической литературы, 1949. 880 с.
5. Руководство для следователей / под общ. ред. В. В. Мозякова. М.: Издательство «Экзамен», 2005. 912 с.
6. Справочник следователя. Осмотр места происшествия / под ред. И. А. Попова. М.: ЦОКР МВД России, 2010. 302 с.

Alexander A. Belyakov

Doctor of Law, Professor, Head of the Department of Criminalistics
Ural State Law University
(Russia, Yekaterinburg)
aleks-1@inbox.ru

Dmitry V. Bakhteev

PhD in Law, Associate Professor of the Department of Criminalistics
Ural State Law University
(Russia, Yekaterinburg)
dmitry.bakhteev@gmail.com

**MOBILE GUIDE OF THE INVESTIGATOR: CONTENT AND TECHNICAL
CONDITIONS**

Abstract: The paper discusses the form and content of the mobile guide as a tool of information support of investigative activities. The technical requirements for such applications, a typical structure are given.

Keywords: Crimlib.info, reference book of the investigator, mobile reference book, informatization.

Брунцов Андрей Сергеевич
Студент Института юстиции
Уральский государственный юридический университет
(г. Екатеринбург)
grittings@mail.ru

ТЕХНОЛОГИЯ СОБИРАНИЯ, ИССЛЕДОВАНИЯ И ИСПОЛЬЗОВАНИЯ СМС И ПЕРЕПИСОК В МЕССЕНДЖЕРАХ И СОЦИАЛЬНЫХ СЕТЯХ КАК ДОКАЗАТЕЛЬСТВА В СУДЕБНОМ РАЗБИРАТЕЛЬСТВЕ

Аннотация: в статье рассматривается процесс собирания, исследования и использования СМС-сообщений и переписок в мессенджерах и социальных сетях, его применение на практике и проблемные аспекты, связанные с данным процессом.

Ключевые слова: мессенджеры, социальные сети, использование доказательств, судебный процесс, переписка.

По мере того, как происходит развитие науки и техники, совершенствуются вместе с ними и различные способы передачи информации от одного лица к другому. С завидной частотой создаются разработки, позволяющие улучшать, ускорять и облегчать процесс взаимодействия людей между собой. К большому сожалению, не так уж редко эти новые технологии используются гражданами в общественно-неполезных целях, а зачастую они изначально разрабатываются для того, чтобы скрывать противоправные деяния или иным образом обходить закон. В связи с этим у законодателя и правоприменителя порой возникает не очень легкая задача – успевать не только реагировать на такие нововведения в обществе, но и делать это правильно, в рамках закона, чтобы нормативная правовая база могла соответствовать передовым технологиям, а законность использования доказательств, полученных из не совсем обыденных и традиционных источников не вызывала сомнений.

Понятно, что электронные доказательства могут содержаться на самых различных носителях – будь то флеш-карты, жесткие диски, серверы и прочее, но все же в современных условиях наиболее актуальным, на мой взгляд, будет разговор о том, каким образом правильно собрать, исследовать и использовать СМС-сообщения, а также сообщения в различных мессенджерах и социальных сетях, коих в наше время развелось достаточно много.

Довольно длительный промежуток времени вопрос о том, возможно ли использовать в судебном разбирательстве переписку по СМС или же в мессенджерах, например, What's App, Telegram, Viber, оставался открытым, но на сегодняшний день суды, вроде бы, пришли к единому мнению – если все сделать в рамках закона и с соблюдением материальных и процессуальных норм, то такое доказательство может являться вполне допустимым¹.

Последними изменениями в ч.1 ст. 71 ГПК РФ как раз-таки были внесена возможность использовать материалы, полученные в том числе с помощью информационно-телекоммуникационной сети «Интернет», либо выполненные иным

¹ Постановление Арбитражного суда Уральского округа от 18 ноября 2016 г. N Ф09-9930/15 по делу N А50-7834/2015, Постановление Второго арбитражного апелляционного суда от 5 марта 2018 г. N 02АП-606/18, Постановление Девятого арбитражного апелляционного суда от 15 ноября 2017 г. N 09АП-50243/17, Постановление Пятнадцатого арбитражного апелляционного суда от 28 октября 2015 г. N 15АП-17545/15.

позволяющим установить достоверность документа способом¹. Аналогичная норма была закреплена ранее и в ст. 75 АПК РФ².

То есть теперь более интересен вопрос не о том, разрешено ли вообще использовать подобного рода переписку как доказательство, а именно вопрос, каким образом использовать ее грамотно, законно и максимально полезно для дела? Вообще варианта, как таковых, два: первый из них – обеспечение доказательств с помощью нотариуса, второй – закрепление доказательств самостоятельно.

Если идти по первому пути, то такое обеспечение производится в порядке, который закреплен ст. ст. 102–103 Основ законодательства о нотариате³. Здесь нотариус, по сути, сделает то, что относится к компетенции суда, то есть произведет осмотр телефона, составление протокола, и эти действия, само собой, будут соответствовать всем требованиям, предъявляемым законом. Но важно понимать, что нотариус заверяет не тот факт, что именно какой-либо конкретный человек написал данное сообщение с этого телефона, а тот факт, что это сообщение в принципе присутствует, что само по себе несколько не увеличивает шансы доказать в суде связь между сообщением и его отправителем. Тут уже все будет зависеть именно от того, насколько убедительно одна из сторон свяжет факт наличия данного сообщения с его принадлежностью к конкретному лицу.

Если говорить о недостатках такого способа, то к ним относятся сравнительная дороговизна и потеря некоторого количества времени и сил на поиски нотариуса, который бы согласился заверить такую информацию и на само ее заверение. Но зато в случае успеха суд не сможет отказать в принятии такого доказательства лишь по формальным мотивам, а именно по мотиву несоответствия формы доказательства закону.

Второй путь – это оформление переписки самостоятельно. Чётких правил здесь уже нет, вследствие чего каждый делает так, как считает правильным. Кто-то заверяет так называемые «скриншоты», кто-то перепечатывает текст сообщения на бумажный носитель и пытается представить его суду в таком виде, но какой бы вариант ни выбрал гражданин, все равно для подтверждения факта переписки и удостоверения ее правильности придется предоставить суду сам телефон, с которого велась переписка. Если этого не сделать, то сила всех приложенных «доказательств» аннулируется со стопроцентной вероятностью. И вот тут мы сталкиваемся с одним из основных камней преткновения – что, если физически телефона уже не будет либо сообщение будет удалено по любой причине: специально, по ошибке, из-за вируса и так далее? Тогда доказательство как таковое просто перестает существовать! И даже в том случае, если в реальности оно и сохранилось!

Но это еще не самая главная проблема. Куда более явным недостатком данной системы является, на мой взгляд, другая вещь. Всем известно, что с недавних пор во всех мессенджерах можно удалять из диалога отправленные вами сообщения. В основном, такая возможность предоставляется в течение 24 часов с момента отправки сообщения, но этого вполне достаточно, чтобы быстро довести до сведения адресата какое-либо противоправное послание и избавиться от него за считанные секунды! Причем если где-то, например, в What's App или Instagram собеседник узнает, что сообщение было удалено его отправителем, то во ВКонтакте или Telegram он об этом даже не догадается, если не увидит «исчезновение» своими глазами. По моему мнению, вопрос о том, как быть с подобного рода вполне легальным «избавлением от следов преступления» должен стоять намного более остро, чем проблема правильного преподнесения этих доказательств в суде с точки зрения соблюдения всех формальностей.

¹ Изменения внесены Федеральным законом от 23 июня 2016 г. N 220-ФЗ и вступили в силу с 01.01.2017 г.

² Арбитражный процессуальный кодекс Российской Федерации от 24.07.2002 N 95-ФЗ (с изм. и доп., вступ. в силу с 25.12.2018).

³ Основы законодательства РФ о нотариате от 11 февраля 1993 г. N 4462-I.

Возможно, создателям мессенджеров и социальных сетей следует организовать какую-либо «базу удаленных сообщений» каждого пользователя, доступ к которой можно было бы получить лишь по судебному решению, чтобы не было нарушено конституционное право человека и гражданина на тайну переписки? Или, может быть, совсем убрать возможность удаления или редактирования отправленных сообщений? Но тогда это вызовет волну недовольств и протестов со стороны добропорядочных граждан. Каким бы ни был выход, но решать этот вопрос, на мой взгляд, необходимо, потому что жизнь все более быстрыми темпами перебирается на пространство Интернета. Если говорить о последствиях на уголовно-правовом поле, то в связи с этим развивается киберпреступность, растет количество приготовлений к преступлениям именно путем обсуждения каких-либо моментов в защищенных мессенджерах, а неспособность законодателя быстро отреагировать на такие изменения может привести к серьезному росту преступлений, совершаемых подобным образом. Если же рассуждать относительно гражданско-правовых отношений, то подобная ситуация тоже ничего хорошего не сулит, ведь из-за таких возможностей можно потерять массу доказательств, способных потенциально стабилизировать отношения в обществе.

Если предположить ситуацию, когда переписка была удостоверена в соответствии с законом, суд ее принял в качестве надлежащего и допустимого доказательства по делу, то на этом работа не заканчивается, а наоборот, начинается самая основная задача – доказать, что данные сообщения были присланы именно тем лицом, на которое вы указываете. И здесь мы сталкиваемся с еще одной немаловажной проблемой – как это сделать? Если речь идет об СМС-переписке или сообщениях в мессенджере, который привязан непосредственно к номеру телефона, то здесь можно будет запросить нужные сведения у оператора сотовой связи. Но как быть, если телефон оформлен совсем на другое лицо или организацию? Здесь уже необходимо прибегать к косвенным доказательствам. Может быть, лицо само представится в переписке, возможно, что этот телефон будет указан в официальных документах лица, одним словом, нужно проявить изобретательность и постараться доказать причастность любыми законными способами.

А если переписка происходит в социальной сети, например, ВКонтакте? Тогда шансы доказать, что именно конкретный человек отправлял данное сообщение фактически сводятся к нулю, поскольку страница не привязывается ни к паспорту, ни к настоящему имени, плюс возможен фактор взлома, рассылки различного рода сообщений и так далее.

В настоящее время в Государственной Думе рассматривается так называемый закон «О социальных сетях», одним из пунктов которого является обязательство указывать паспортные данные/иные удостоверяющие личность документы при регистрации личного аккаунта в социальных сетях. Я считаю, что как раз хотя бы для частичного решения проблемы «привязки» отправленного сообщения к конкретному человеку данный закон будет весьма кстати. Конечно, здесь так же останется вероятность взлома аккаунта и прочих непредсказуемых вещей, но все же это нововведение позволит намного сузить перечень вопросов, которые возникают при использовании доказательств, связанных с перепиской в соц. сетях в суде.

И последняя проблемная зона, которую я хотел бы затронуть в данной работе, это содержание обсуждаемых сообщений. Не секрет, что зачастую при написании сообщений стороны используют какие-либо сокращения, кодовые слова, жаргонизмы, диалектизмы и прочие прелести великого и могучего. Не всегда такие сообщения ясны и понятны обывателю, а также судье или следователю. Например, в Постановлении Восьмого арбитражного апелляционного суда от 17 января 2017 г. N 08АП-13836/16¹ суд указал, что «Из содержания переписки не следует, какие именно документы, кто и у кого запрашивал, какая именно ситуация является предметом переписки (нет описаны обстоятельства

¹ Постановление Восьмого арбитражного апелляционного суда от 17 января 2017 г. N 08АП-13836/16.

утраты груза, реквизиты судна, капитан, договор и т.п.). Переписка не подтверждает факт передачи груза ответчику». В данном случае речь как раз идет о неполной и не очень понятной суду переписке. Решением такой проблемы, на мой взгляд, будет назначение лингвистической экспертизы и установление смысла исследуемых переписок, которые уже в понятном для всех виде будут переданы суду и сторонам.

Таким образом, исходя из всех ранее проанализированных фактов, можно сделать несколько выводов: во-первых, переписка по СМС, в мессенджерах или в социальных сетях, без сомнений, может использоваться в качестве доказательств по делу в судебных разбирательствах. Во-вторых, фиксировать данную переписку желательно у нотариуса, чтобы избежать проблем в дальнейшем, но переписка, закрепленная самостоятельно тоже при определенных обстоятельствах может быть принята судом. В-третьих, необходим подробный лингвистический анализ самой сути переписки и устранение каких-либо смысловых пробелов в ней. И в-четвертых, существует несколько проблем, связанных именно с использованием уже удаленных фактически сообщений, а также с определением принадлежности посланного сообщения конкретному лицу. Как раз-таки укрепление слабых мест, на мой взгляд, должно стать приоритетной задачей законодателя, поскольку это позволит вывести процесс, связанный с собиранием, исследованием и использованием СМС-переписок, переписок в мессенджерах и социальных сетях на совершенно новый уровень, который будет соответствовать современным реалиям и, несомненно, улучшит и стабилизирует общественные отношения.

Список литературы

1. Ермакова Е. С., Джумангалиева Д. М. Электронные доказательства как новое направление в практике расследования преступлений // Молодой ученый. 2018. № 23. С. 85-87. Режим доступа: <https://moluch.ru/archive/209/51196/>.
2. Ефремов И. А. О достоверности электронных документов при осуществлении уголовного судопроизводства // Информационное право. 2006. № 2.
3. Зигура Н. А. Компьютерная информация как вид доказательств в уголовном процессе России: автореф. дис.... канд. юрид. наук. Челябинск, 2010. 20 с.

Andrei S. Bruntsov
Student of Institute of Justice
Ural State Law University
(Russia, Yekaterinburg)
grittings@mail.ru

TECHNOLOGY OF COLLECTING, RESEARCHING AND USING SMS AND CORRESPONDENCE IN MESSENGERS AND SOCIAL NETWORKS AS EVIDENCE IN COURT PROCEEDINGS

Abstract: The article discusses the process of collecting, researching and using SMS messages and correspondence in messengers and social networks, its practical application and problematic aspects associated with this process.

Keywords: Messengers, social networks, use of evidence, litigation, correspondence.

Галиханова Карина Ришатовна

Студент Института государственного и международного права
Уральский государственный юридический университет
(г. Екатеринбург)
kaj230398@mail.ru

Рачева Нелли Витальевна

Кандидат юридических наук, доцент, доцент кафедры криминалистики
Уральский государственный юридический университет
Екатеринбург
ekaterinburg@mail.ru

**ИСПОЛЬЗОВАНИЕ БЕСПИЛОТНЫХ ЛЕТАТЕЛЬНЫХ АППАРАТОВ В
ДЕЯТЕЛЬНОСТИ ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ**

Аннотация: В настоящее время почти каждая сфера деятельности человека стремится к автоматизации, тем самым делая жизнь людей более удобной и продуктивной. Использование беспилотных летательных аппаратов в работе правоохранительных органов способствует более оперативному и качественному раскрытию и предотвращению преступлений. Однако не стоит забывать, что такой «робот» не всегда сможет заменить человека.

Ключевые слова: беспилотные летательные аппараты; БПЛА; правоохранительные органы; транспортная инфраструктура, преступления.

Изобретение прототипов первых БПЛА можно связать с появлением радио и электричества. Уже в середине XIX века (а именно в 1849 году) во время Австро-Венгерского вооруженного конфликта Австрия применила бомбардировочные аэростаты с борта военного корабля. В 1897 году Николаем Тесла был получен патент по применению беспроводной передачи для управления дирижаблем. В 1899 он представил модель радиоуправляемого корабля. Свой расцвет БПЛА получили во времена Второй мировой войны. Германия, США, Великобритания не смогли обойти стороной их применение. Особый «успех» получили управляемые бомбы Henschel Hs 293 и Fritz X, а также «самолеты-снаряды» ракета Фау-1 и ракета Фау-2. СССР, главный авиаконструктор периода Второй мировой войны выказывал попытки воплотить в жизнь постройку беспилотной ракеты с дальностью полета от 100 км и скоростью в 700 км/ч, но задумку ему воплотить не удалось. Однако во время ведения войны был применен тяжелый бомбардировщик ТБ-3 в качестве беспилотного самолета для подрывов мостов.

Чтобы сформировать точное понимание термина беспилотный летательный аппарат, необходимо обратиться к Постановлению Правительства РФ от 11.03.2010 N 138 "Об утверждении Федеральных правил использования воздушного пространства Российской Федерации", в котором сказано, что беспилотный летательный аппарат - это летательный аппарат, выполняющий полет без пилота (экипажа) на борту и управляемый в полете автоматически, оператором с пункта управления или сочетанием указанных способов (далее – БПЛА).

Существуют различные классификации БПЛА, но наиболее используемые из них являются:

По размеру БПЛА:

- микро БПЛА (время нахождения в воздухе – 60 минут; вес – менее 10 кг; высота нахождения в воздухе – до 1 км);

- мини БПЛА (время нахождения в воздухе – до 5 часов; вес – около 50 кг; высота нахождения в воздухе – 3-5 км);
- миди БПЛА (время нахождения в воздухе – 15 часов; вес – до 1 тонны; высота нахождения в воздухе – до 10км);
- тяжелые БПЛА (время нахождения в воздухе – более суток; вес – более 1 тонны; высота нахождения в воздухе – 20 км).

По виду и назначению:

- беспилотные самолеты (используются правоохранительными органами для мониторинга площадных и линейный территорий) (см. Илл. 1);



Беспилотный самолёт. Фотография с сайта <https://ot-vinta.org/belorusskij-zavod-povez-na-vystavku-svoi-bespilotniki/>

- беспилотные вертолеты (мониторинг локальных участков местности, так как данным БПЛА не нужна взлётно-посадочная полоса, сами по себе легкие и небольшие);



Беспилотный вертолёт. Фотография с сайта https://www.equipnet.ru/articles/hi-tech/hi-tech_1478.html

- беспилотные аэростаты (могут опускаться для мониторинга на высоту до 400 метров, работают долгое время без подзарядки):

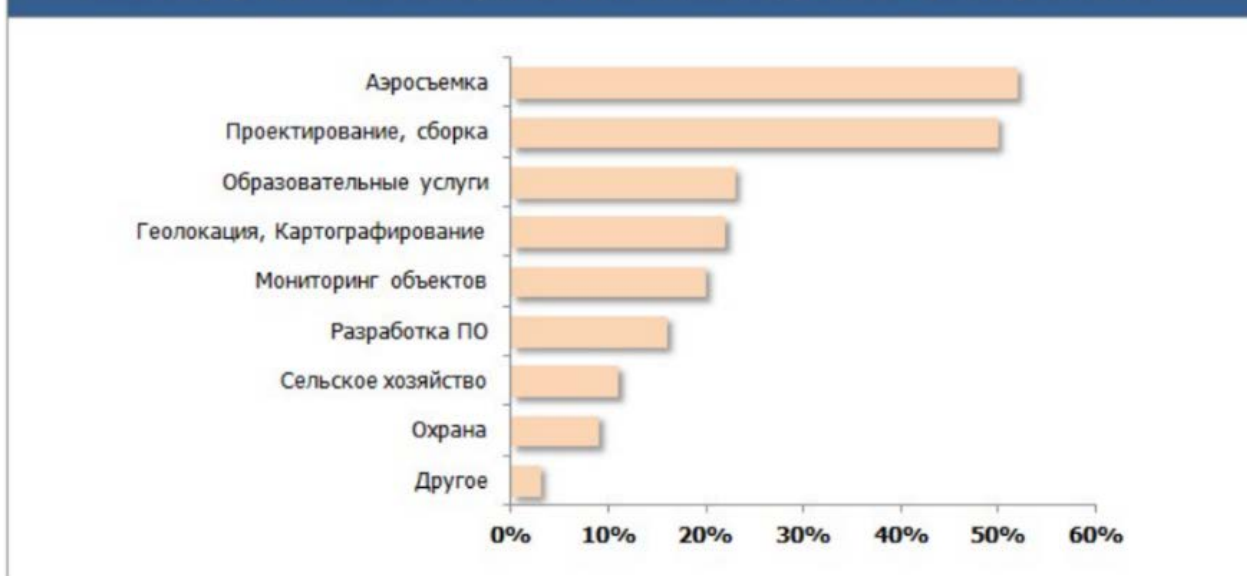


Беспилотный аэростат. Фотография с сайта <https://северная-линия.рф/2013/11/01/дирижабль-на-защите-природных-ресурс/>

Хотя распространено мнение, что БПЛА в большинстве случаев применяются как средства военной техники, их использование помогает человеку еще, как минимум, в пяти сферах деятельности: при возникновении чрезвычайных ситуаций и чрезвычайных

происшествий БПЛА применяются для их предупреждения, для поиска людей и проведения спасательных операций, тушение пожаров; для обеспечения безопасности людей и объектов (их охрана и обнаружение); мониторинг и наблюдение за необходимыми для жизнеобеспечения человека протяженными установками, а также за природными ресурсами (ЛЭП, АЭС, водные и лесные ресурсы, нефтегазовые ресурсы и т.д.); для аэрофотосъемки больших территорий с воздуха (картография, геодезия); для научных исследований и открытий в местах труднодоступных для человека (исследование Арктики, научно-исследовательские и опытно-конструкторские работы).

Рис. 2. Сферы деятельности российских компаний, работающих на рынке БПЛА



Источник: Ассоциация БПЛА

В коммерческих структурах БПЛА тоже являются активно внедряемой новацией. Так, в июне 2017 года БПЛА успешно доставил наличные денежные средства из отделения Сбербанка до машины инкассаторов. При этом скорость БПЛА была 180 км/ч. Но для дальнейшего использования БПЛА в банковской деятельности необходимо разрешение Центрального Банка России. Логистическая компания Matternet в Швейцарии получила разрешение на транспортировку крови и образцов анализов между больницами и медицинскими центрами страны. Данная перевозка занимает до получаса по времени, что помогает сохранить образцы для проведения лабораторных анализов и для проведения операций. В Сингапуре БПЛА используются, как летающие такси. БПЛА так же активно используют такие популярные корпорации, как Mercedes-Benz, «Газпром нефть», Google, Facebook. Планируется их использование Почтой России.

Интересным фактом является то, что по оценке J'son & Partners Consulting¹ только 10 % территории Российской Федерации обеспечено сотовой связью. По данным Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации, сотовая связь есть почти во всех населённых пунктах РФ, но 1343 городских поселения с численностью жителей от 10 тыс. до 500 тыс. остаются без доступа к Интернету и мобильной связи. Еще 38 %, или 6725 населенных пунктов составляют города и села, где есть голосовая сотовая связь, но отсутствует как проводной, так и беспроводной доступ в Интернет. Поэтому сейчас для получения услуг связи за пределами зон покрытия сотовых сетей, особенно в труднодоступных районах, как правило, используется спутниковая связь. Тарифы на спутниковую связь и передачу

¹ J'son & Partners Consulting - международная консалтинговая компания, специализируется на рынках телекоммуникаций, медиа, ИТ, инновационных технологиях в России, СНГ, Центральной Азии. Действует с 1996 года.

данных намного выше тарифов сотовых операторов, так как проектирование спутников, их запуск и обслуживание требуют огромных инвестиций.

Одним из решений данной проблемы является внедрение в деятельность операторов связи привязных дронов. Данные БПЛА оснащены легким кабелем, с помощью которого в систему дронов подается напряжение, позволяющее им находиться в подвешенном состоянии неограниченное количество времени. Кроме того, такие дроны смогут обеспечивать сотовой связью и Интернетом обширные участки территорий.



Дрон Aquila, (2017)

Использование БПЛА напрямую не предусмотрено при выполнении следственных действий или оперативно-розыскных мероприятий. Однако, в ст. 164 Уголовно-процессуального Кодекса Российской Федерации и ст. 6 Федерального закона от 12.08.1995 № 144-ФЗ «Об оперативно-розыскной деятельности» закреплено применение технических средств уполномоченными на то должностными лицами. Использование технических средств не должно наносить ущерб жизни и здоровью человека и причинять вред окружающей среде. Однако, для более детального регулирования правильного применения БПЛА составлен законопроект, который на данный момент находится на рассмотрении Государственной Думы. Данный законопроект предусматривает принятие Федерального закона Российской Федерации (далее – ФЗ), который внесёт поправки в ряд нормативных актов, в частности, в ФЗ «О федеральной службе безопасности», в ФЗ «О государственной охране», в Воздушный кодекс Российской Федерации, в ФЗ «О полиции», в ФЗ «О войсках национальной гвардии Российской Федерации». В измененных нормах планируется установить запрет на несанкционированное использование БПЛА на объектах транспортной (аэро- и морских портов, железнодорожных вокзалов, магистралей и др.), информационной и телекоммуникационной (стационарных и мобильных пунктов государственного управления и др.) инфраструктуры, а также в местах проведения культурно-массовых (концертов, фестивалей, футбольных матчей и др.) и публичных мероприятий, в местах защищенности критически важных объектов (электростанций, химических предприятий др.).

Такая необходимость обусловлена тем, что БПЛА используются не только для совершения преступлений (например, как средство доставки взрывных устройств и легковесного оружия, распыления отравляющих веществ в местах массового пребывания

людей, распространения наркотиков, контрабанды, для передачи информации и запрещенных объектов лицам, отбывающим наказание в местах лишения свободы), но и могут создавать помехи в деятельности объектов транспортной инфраструктуры. Например, 06.07.2016 в Тульской области в Государственном музее-заповеднике «Куликово поле» БПЛА выполнял несанкционированный полет на недопустимо малой высоте, из-за этого возникла опасность причинения вреда группе детей, которые посещали музей с экскурсией; 09.05.2017 в Хабаровске пресекли несанкционированный полёт БПЛА, который подлетел к группе самолетов, выполнявших демонстрационные манёвры на параде, посвященном празднованию Дня Победы (самолеты были вынуждены остановиться).

В РФ 03.07.2016 был разработан разрешительный порядок использования БПЛА. Порядок установлен Воздушным Кодексом Российской Федерации, в котором закреплено обязательное соблюдение учёта беспилотных летательных судов с максимальной взлетной массой от 0,25 килограмма до 30 килограммов¹. Во исполнении данного Федерального закона Российской Федерации были разработаны Федеральные правила использования воздушного пространства Российской Федерации, утвержденные постановлением Правительства Российской Федерации от 11.03.2010 № 138. Учётом БПЛА массой от 0,25 кг до 30 кг занимается Федеральное государственное унитарное предприятие «Защита Инфо Транс», подведомственное Министерству транспорта Российской Федерации. Владельцам БПЛА свыше 30 кг необходимо пройти регистрацию в Федеральном агентстве воздушного транспорта. К заявлению на регистрацию необходима квитанция об оплате государственной пошлины (она составляет 350 рублей) и правоустанавливающие документы на беспилотный аппарат. Кроме этого, для полета любого БПЛА массой свыше 0,25 кг необходимо разрешение для использования воздушного пространства. Заявление подаётся в центры Единой системы организации воздушного движения Российской Федерации вместе с представленным планом полёта воздушного судна. При невыполнении данных требований российским законодательством налагается ответственность, в частности, в части 3 ст. 11.5 Кодекса Российской Федерации об административных правонарушениях предусмотрены административный штраф в размере от двух тысяч до двух тысяч пятисот рублей либо лишение права управления воздушным судном на срок до одного года.

Как отмечалось выше, с помощью БПЛА совершается немало преступлений: контрабанда наркотических средств, психотропных веществ и их аналогов, транспортировка запрещенных или ограниченных в гражданском обороте средств в места лишения свободы и террористические акты. Так, 4 августа 2018 года, в ходе выступления на параде венесуэльского президента Николаса Мадуро, в отношении президента было совершено покушение на убийство с использованием дронов. Несколько БПЛА летели с взрывчаткой С-4 (по килограмму на каждом) и должны были взорваться рядом с президентом Венесуэлы. Но все дроны были вовремя замечены и подбиты снайперами полиции Венесуэлы.

В Российской Федерации с 2016 года началась активная попытка внедрения БПЛА в деятельность правоохранительных органов, и с каждым годом их количество в подразделениях органов охраны порядка только растет. Согласно данным, опубликованным Федеральным агентством воздушного транспорта, в 2016 году было введено более 1 млн БПЛА, а по прогнозу некоммерческого партнерства «ГЛОНАСС» это количество к 2025 году может увеличиться в 100 раз. Ярким примером эффективности БПЛА служит их применение для выявления нарушений Правил дорожного движения. Приказ МВД России от 23.08.2017 N 664 уже содержит нормы, позволяющие использовать БПЛА в качестве средства по надзору за дорожным движением.

¹ Статья 33 Воздушного кодекса Российской Федерации от 19.03.1997 N 60-ФЗ

Красноярский край стал одним из первых субъектов РФ, где БПЛА начали применяться на постоянной основе. БПЛА с высоты 500 метров фиксирует всё, что происходит на дороге и передаёт видеоизображение на наземный пункт управления онлайн. При обнаружении дорожного правонарушения БПЛА преследует автомобиль до остановки его инспектором. Кроме этого, БПЛА является незаменимым средством для поиска угнанных автомобилей или при попытке автомобиля скрыться с места происшествия. БПЛА на дорогах – оперативный способ сократить и предотвратить число преступлений. БПЛА является эффективным способом для постоянного контроля протяжённых, часто неохраняемых в труднодоступных зонах участков железных дорог, водных акваторий, трубопроводов, полевых пространств, участков лесных пространств. Исходя из новостей информационного портала «iot», в 2016 году в Республике Адыгея БПЛА помогли выявить 150 дорожных нарушений. Все нарушения были связаны с выездом на полосу встречного движения, что является одним из самых опасных нарушений ПДД.

БПЛА являются незаменимыми средствами для поиска людей при их похищении или пропаже, для перехвата транспортировки наркотических средств, психотропных веществ и их аналогов, для расследования побегов заключённых. БПЛА помогают выявить кражу дорогостоящих биоресурсов или лесоматериалов при их транспортировке. В последнее время, когда мир всё чаще сталкивается с совершением террористических актов, БПЛА помогают проводить непрерывный мониторинг площадей с большим скоплением людей - метро, железнодорожных путей и иных путей транспортного сообщения для заблаговременного предупреждения преступлений. БПЛА являются отличными помощниками для осмотра места происшествия, причем в их деятельности применяются почти такие же методы, как и следственно-оперативной группой. Для общего осмотра территории наиболее целесообразным является кольцевой маршрут. Достоинством этого метода является охват большой территории, оперативность и быстрота, относительно простое планирование полетного задания и оперативная обработка полученных результатов. Для детального осмотра участков местности в пределах рабочей зоны применяются прямолинейные взаимно параллельные маршруты

Для содействия в борьбе с БПЛА, с помощью которых совершаются преступления, правоохранительные органы используют свои БПЛА. Для поиска дронов преступников задействованы системы, способные распознать запуск коптеров по радиосигналу (например, в Москве данная система расположена на Останкинской телебашне) либо возможно использовать цифровые городские камеры. После обнаружения БПЛА нарушителя для его ликвидации может помочь БПЛА правоохранительных органов. Такой БПЛА способен подавить радиосигнал другого дрона и даст возможность принудительно его посадить. В зависимости от заложенной программы, потеряв сигнал, дрон может либо сразу же приземлиться, либо попробовать вернуться в точку отправления. Также есть иные методы предотвращения полета дронов-нарушителей.



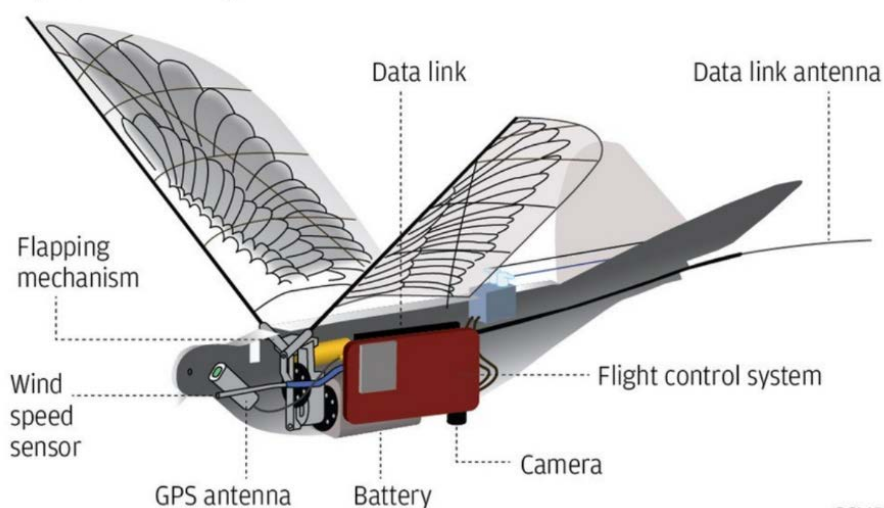
Отлавливание дрона-нарушителя. Источник: 3dnews.ru

В 2013-2015 годах у Военно-морского флота постепенно сформировался свой «беспилотный полк». Воинские части на Камчатке, в Крыму и в Североморске оснащены БПЛА «Форпост» и «Орлан-10». Причем данные БПЛА используют не только для военных целей (наведение артиллерии и авиации, военная разведка), но и для помощи правоохранительным органам в мирное время (поиск людей, терпящих бедствие на море, патрулирование прибрежных территорий и слежение за экологической обстановкой).

Интересно, что до декабря 2017 года Полиция Нидерландов использовала специально обученных орлов для ликвидации запрещенных дронов. Проект не смог реализоваться из-за сложности обучения птиц и дороговизны их содержания. Предполагалось, что орлы при обнаружении запрещённого БПЛА должны были перехватывать их и уносить в определенное место. Но из-за особенности поведения животного команда не всегда выполнялась, появлялась угроза причинения вреда не только людям, но и самим орлам лопастями дрона.

Правоохранительные органы Китая в июне 2018 года стали использовать дроны для контролирования порядка населения. БПЛА были замаскированы под голубей, чтобы не смущать жителей городов. Радиоуправляемые БПЛА, которые являются частью программы под названием «Голубь» (Dove), уже используются военными организациями и органами власти в пяти провинциях Китая.

Eye in the sky



SCMP

Робот-голубь в Китае



Запущены роботы-голуби для слежки за населением

Дроны программы «Голубь». Фотографии с сайта <http://www.tadviser.ru/>

В завершении, необходимо отметить, что БПЛА так же активно применяются при ведении войны или при возникновении вооруженных конфликтов. Применение БПЛА в данном случае подчиняется праву вооруженных конфликтов (*jus ad bellum* и *jus in bello*), их использование должно быть необходимым и соразмерным, их действие должно быть направлено только против военных объектов и комбатантов. По опыту вооруженных сил, правоохранительные органы Российской Федерации могут в скором времени перенять применение поражающих свойств БПЛА в своей деятельности. С одной стороны, такое применение БПЛА могло бы предотвратить множество преступлений, в особенности террористические акты. С другой стороны, данные аппараты могли бы обеспечить сохранность жизни и здоровья сотрудников правоохранительных органов. Однако, применение БПЛА в деятельности правоохранительных органов должно лишь продолжать «содействовать» раскрытию и предотвращению преступлений.

Использование поражающих свойств БПЛА, с помощью которых можно атаковать человека и нанести вред его здоровью или жизни, создает опасность нанесения вреда большего, чем предотвращенного. В частности, на объектах транспортной инфраструктуры почти всегда сосредоточено большое скопление людей, а применение поражающих свойств БПЛА создает опасность причинения вреда невинному населению; самостоятельность автоматизированных БПЛА может практически исключать присутствие человека при принятии ими решений, что создает опасность применения прагматичного, безнравственного решения. Кроме того, БПЛА являются несовершенными в обнаружении статических целей, особенно в обустроенных городах и лесистых местностях; отдаленное присутствие человека от места происшествия может вызвать в нём чувство безучастия. Наблюдение сотрудника правоохранительных органов за преступлением через экран монитора может вызвать в нём «эффект компьютерной игры», что недопустимо при принятии таким сотрудником решений, имеющих юридическое значение для других лиц.

Список литературы

1. Автономные военные БПЛА перестали быть научной фантастикой // Вестник НАТО [Электронный ресурс]. Дата обновления: 28.07.2017. Режим доступа: <https://www.nato.int/docu/review/2017/Also-in-2017/autonomous-military-drones-no-longer-science-fiction/RU/index.htm>.

2. Беспилотный летательный аппарат БПЛА (дрон) // TADVISER Государство. Бизнес. ИТ. [Электронный ресурс]. Дата обновления: 27.03.2019. Режим доступа: [http://www.tadviser.ru/index.php/Статья:Беспилотный_летательный_аппарат \(дрон,-БПЛА\)](http://www.tadviser.ru/index.php/Статья:Беспилотный_летательный_аппарат_(дрон,-БПЛА)).

3. Котарев С. Н., Котарева О. В., Александров А. Н. Использование беспилотных летательных аппаратов для обеспечения безопасности на объектах транспорта // Вестник Восточно-Сибирского института МВД России. 2017. № 5. С.27-31.

4. Стрижевский Д. А. Повышение безопасности дорожного движения на основе развития системы мониторинга автомобильных дорог // Инновации и исследования в транспортном комплексе: междунар. науч.- практ. конф. Курган, 2013. С. 255-261.

Karina R. Galikhanova

Student of Institute of State and International Law

Ural State Law University

(Russia, Yekaterinburg)

kaj230398@mail.ru

Nelli V. Racheva

Ph.D. Associate Professor

Ural State Law University

(Russia, Yekaterinburg)

ekaterinburg@mail.ru

USE OF UNMANNED AIRCRAFT SYSTEMS IN THE ACTIVITIES OF LAW ENFORCEMENT ACTIVITIES

Abstract: Nowadays, almost all areas of human activities are aimed at automation. The use of unmanned aerial vehicles in work processes enables more operative and efficient solving and prevention of crimes, however, one should not forget that such a ‘robot’ will not always be able to replace a human being.

Keywords: unmanned aerial vehicles (UAV), law-enforcement agencies, transport infrastructure.

Дерюгин Роман Александрович

Кандидат юридических наук, преподаватель кафедры криминалистики
Уральский юридический институт МВД России
(г. Екатеринбург)
deryugin.r.a@mail.ru

Жижилева Анастасия Александровна

Курсант Факультета подготовки следователей
Уральский юридический институт МВД России
(г. Екатеринбург)
zhizhileva74@mail.ru

**ПЕРСПЕКТИВЫ РАЗВИТИЯ ЦИФРОВОЙ КРИМИНАЛИСТИКИ В УСЛОВИЯХ
ИНФОРМАЦИОННОГО ОБЩЕСТВА**

Аннотация: В статье рассмотрены тенденции развития цифровой криминалистики в условиях совершенствования и расширения возможностей сети Интернет, мобильных приложений, в частности приложений-мессенджеров и распространения криптовалют. Авторы исследуют вопросы, связанные с использованием виртуальных (электронных) следов в процессе деятельности по раскрытию и расследованию преступлений.

Ключевые слова: информационные технологии, Интернет, криптовалюта, «фейковая» информация, электронные следы, виртуальные следы, цифровая криминалистика.

21 век ассоциируется с богатым набором прорывных технологий. Развитие и внедрение новых информационно-телекоммуникационных технологий, а также создание на их основе компьютерной техники, повсеместное ее внедрение во все сферы человеческой жизни – основное направление цифровизации общественных отношений. Криминалистика не осталась в стороне от этого процесса, и последнее время все так же активно трансформирует в науку новые знания и технические новшества, связанные с собиранием, исследованием и оценкой вещественных доказательств, полученных в рамках раскрытия и расследования преступлений. При этом, есть и негативные стороны прогресса. Так, бурное развитие информационных технологий поставило под угрозу эффективную защиту прав человека. Сегодня возможно искать, получать и передавать информацию независимо от государственных границ – благодаря использованию ресурсов Интернета. В настоящий момент предпринимаемые попытки законодательно урегулировать использование информационных технологий часто сопряжены с нарушением фундаментальных прав человека.

Интернет для современного человека является незаменимой составляющей полноценной жизни и основой взаимодействия в обществе. Сеть Интернет специально ориентирована на поиск, получение, хранение, распространение информации, нужной конкретному лицу. Человек под влиянием информационной среды видоизменил сущность гарантий реализации отдельных конституционно-правовых положений, в частности, по привлечению граждан в управлении делами на благо государства. В связи с этим, большая часть правовых гарантий по реализации информационного права требует серьезного анализа и совершенствования, для того, чтобы соответствовать «требованиям» информационной среды.

18 марта 2019 года был принят Федеральный закон № 31-ФЗ «О внесении изменений в статью 15.3 Федерального закона «Об информации, информационных технологиях и о защите информации», суть которого заключается в организации запрета

на распространение недостоверной, но общественно значимой информации.

Законом определено, что следует понимать под «недостоверной общественно значимой информацией» – информация, которая угрозу причинения вреда жизни и (или) здоровью граждан, имуществу, угрозу массового нарушения общественного порядка и (или) общественной безопасности, либо угрозу создания помех функционирования или прекращения функционирования объектов жизнеобеспечения, транспортной или социальной инфраструктуры, кредитных организаций, объектов энергетики промышленности или связи¹.

Выделяется ряд критериев, которым должна соответствовать недостоверная («фейковая») информация:

- сведения не соответствуют реальной действительности;
- ложные сведения распространяются под эгидой достоверности информации;
- распространяемая информация является общественно значимой;
- создается угроза причинения вреда жизни и (или) здоровью граждан, имуществу и т.п.

Законом определен субъектный состав, которым запрещено распространять «фейковую» информацию в информационно-телекоммуникационных сетях:

- сетевые издания;
- обычные граждане.

Однако, закон специально «обозначает», что ответственность субъекта за совершенное правонарушение должна быть основана на доказанности факта о том, что субъект изначально знал, что распространяет недостоверную информацию.

В 2019 году на рассмотрение в Государственную Думу Российской Федерации был внесен законопроект об изоляции российского сегмента сети Интернет, как ответной меры на опубликованную в 2018 году «Стратегию национальной кибербезопасности США», в целях обеспечения автономной работы российского сегмента сети «Интернет» независимо от мировой глобальной сети. Данный законопроект был инициирован Президентом Российской Федерации В.В. Путиным, который в феврале 2019 года отметил, что создание суверенного рунета является одним из ключевых направлений развития во всем мире.

1 мая 2019 года Президентом Российской Федерации В. В. Путиным был подписан Федеральный закон № 90-ФЗ «О внесении изменений в Федеральный закон «О связи» и Федеральный закон «Об информации, информационных технологиях и о защите информации». Цель данного закона – обеспечение безопасной и устойчивого функционирования сети Интернет. Однако, данный закон начнет свое действие только с 1 ноября 2019 года. К тому же, отдельные нормы, касающиеся криптозащиты информации и национальной системы доменных имен начнут функционировать с 1 января 2021 года. Следует отметить, что из федерального бюджета было выделено 30,8 млрд рублей на обеспечение реализации безопасного, устойчивого рунета в рамках программы «Информационная безопасность».

На наш взгляд, в интерпретации данного федерального закона логично заменить слово «суверенный» рунет на «безопасный», ввиду того, что ограничение доступа детей к определенным сайтам рассматривается как превентивная мера, в то же время ограничение интернета для взрослого – действия по обеспечению безопасности. Закон предполагает установку на организацию устойчивого взаимодействия пользователей в интернет пространстве, не касаясь аспектов принудительного ограничения.

Современный человек активно использует в своей повседневной деятельности результаты научно-технического прогресса. Так, большая часть расчетных операций

¹ О внесении изменений в статью 15.3 Федерального закона «Об информации, информационных технологиях и о защите информации»: Федеральный закон от 18.03.2019 № 31-ФЗ // Собрание законодательства РФ. 25.03.2019. № 12. Ст. 1221.

проводится с использованием технических устройств напрямую через сеть «Интернет» (приложения мобильных банков онлайн, «Apple Pay», «Google Pay» и т.п.); коммуникация между людьми обеспечивается не только посредством привычной всем сотовой связи, но и посредством специальных приложений, социальных сетей, приложений-мессенджеров.

К сожалению, положительные аспекты внедрения новых научно-технических разработок зачастую используются в преступных целях. В последнее время преступники весьма активно и эффективно применяют информационно-телекоммуникационное пространство и возможности новых технологий при совершении самых разнообразных преступлений.

Общество, в том числе и криминальная его часть, погружены в виртуальный мир различными способами.

Например, опосредованно, попадая в объективы систем видеонаблюдения, используя мобильные телефоны, дисконтные, дебетовые карты, карты накопления бонусных баллов в магазинах или устанавливая GPS системы.

Кроме того, подавляющее большинство современных устройств, используемых человеком – от мобильных телефонов до смарт-телевизоров, хранят во внутреннем и на внешнем хранилищах информацию о пользователе.

Вышеперечисленные цифровые технологии активно используются для совершения таких преступлений как:

- незаконный оборот наркотических средств и психотропных веществ,
- мошенничество с использованием платежных карт,
- «мобильные» мошенничества, вымогательства,
- захват заложников,
- компьютерные преступления,
- отмывание денежных средств,
- хищения,
- убийства и другие преступления.

Преступники координируют свою деятельность, поддерживают связь в преступной группе, используют при этом технические новшества в процессе совершения и для совершения преступлений, тем самым оставляя электронные следы.

Электронные следы остаются в различных информационных базах данных, например, базах операторов мобильной связи; при использовании кредитных, дисконтных карт, проездных документов, персональных компьютеров, средств сотовой связи и других устройств, ассортимент которых стремительно расширяется.

В связи с этим, современный правоохранитель просто обязан грамотно использовать цифровые следы в интересах установления истины по делу. Выявление, фиксация, расшифровка таких следов способствует раскрытию и расследованию преступлений, в том числе совершаемых в Интернет пространстве.

С тенденцией развития технологий, оцифровки экономической составляющей последнее время все чаще используют валюту, которая «удобна», т.е. мобильна в различных аспектах ее использования. Таким свойствами на сегодняшний день обладает криптовалюта.

Бумажный денежный оборот остается в прошлом – современный человек использует практически большую часть своих денежных активов именно в электронном эквиваленте. В сети Интернет распространено многоаспектное понятие криптовалюты – биткоин, блокчейн и еще несколько сотен видов. Каким образом отличить криптовалюту от обычных стандартных денежных средств? Криптовалюта не имеет собственника – обладателя, каким выступает государство в обеспечении законно легализованной валюты, введенной на территории страны. Любой человек может разработать собственную криптовалюту – для этого необходимы знания в области информационных технологий (создание программного кода, использование соответствующего

программного обеспечения).

Криптовалюту можно рассматривать как определенную цепочку из чисел (21 млн. комбинаций!), которую «видят» персональные компьютеры инвесторов. Криптовалюта ничем не обеспеченный электронный денежный ресурс, однако, ее покупают по реально выгодному курсу. И все же, криптовалюта ограничена в количественном выпуске, вследствие чего она не обесценивается, наоборот, становится дороже.

Следует констатировать, что фактически во всем мире, в том числе и в России, в настоящее время так и не найдены максимально удобные, адекватные способы использования денежных средств в наличной и безналичной формах.

Проблематика законодательного урегулирования криптовалюты остается весьма актуальной, ввиду того, что подобного рода законопроект был на рассмотрении в Государственной Думе Российской Федерации. Президент Российской Федерации В. В. Путин отметил, чтобы законно использовать криптовалюту – ее нужно легализовать¹. Однако, законопроект от 25 января 2018 года так и не нашел одобрения, вследствие чего Министерством финансов было установлено, что криптовалюта – это финансовый оцифрованный актив, который не является законным платежным средством на территории РФ. Впоследствии велись дискуссии относительно законодательного урегулирования криптовалюты.

Однозначно, спустя несколько лет электронные деньги будут считаться самой универсальной валютой, ввиду того, что на сегодняшний день активно распространяется процесс дедолларизации.

Внедрение новой формы криптовалюты (помимо биткоинов др.) – Bakkt обусловило ряд изменений в развитии криптовалюты во всем мире. Так, с момента внедрения Bakkt наблюдается прорыв в развитии и использовании криптовалюты, однако, нарушая анонимность электронного денежного оборота, все же положительным аспектом стоит отметить тот факт, что валюта Bakkt может работать в оффлайн-режиме, т.е. у данной валюты все операции проходят внутри разработанной платформы, что очень удобно как для разработчика, так и для пользователя. Цель создания данной платформы – разработка экономического сегмента рынка, который впоследствии сможет поддерживать конкурентоспособность потребителя рынка оцифрованных денежных активов. Основная особенность криптовалюты Bakkt – инвестор по истечению срока «работы» однодневных фьючерсов получает биткоин, без привлечения способа расчета операции в фиатной валюте. Таким образом, инвестор, заблаговременно обезопасивший себя от возможности потери денежных активов ввиду вероятной волатильности электронного денежного оборота, самостоятельно анализирует изменчивость цены валюты на финансовом рынке.

По нашему мнению, криптовалюта – революционное решение в рамках альтернативной платежной системы, однако, еще рано утверждать о каких-либо тенденциях и приоритетах развития такого направления в экономическом сегменте. Криптовалюта рассматривается как инновационное решение в реформировании ныне существующей финансовой мировой системы экономического пространства, однако, как показывает практика – участились случаи мошеннических действий, связанные с незаконным «отмыванием» криптовалюты в российские рубли и доллары США.

Основным преимуществом криптовалюты выступает тот факт, что заданной деятельностью нет соответствующего контроля, отсутствует контрольно-надзорный орган. Реализация принципа анонимности в использовании криптовалюты в реализации расчетных операций позволяет не использовать свои персональные данные, что с правоохранительной точки зрения порождает латентную преступность ввиду того, что

¹ Филиппова Е. Криптовалюту в России собираются узаконить в первой половине года // Парламентская газета. Экономика. [Электронный ресурс]. Дата обновления: 20.03.2018. Режим доступа: <https://www.pnp.ru/economics/kriptovalyutu-v-rossii-sobirayutsya-uzakonit-v-pervoy-polovine-goda.html> (дата обращения: 18.05.2019).

отсутствует идентификация субъекта – расцветает вариативность совершения мошеннических действий. В ряде стран криптовалютой расплачиваются за незаконный оборот наркотических средств и психотропных веществ.

Сказанное свидетельствует о необходимости развития цифровой криминалистики как отдельного направления криминалистической науки. И, очевидно, данный факт обусловлен не только научно-техническим прогрессом, но и требованиями правоприменительной практики.

На сегодняшний день цифровая криминалистика как система знаний находится на стадии формирования. Вместе с тем достигнутый уровень развития направлений цифровой криминалистики позволяет уже сейчас обеспечить раскрытие и расследование особо сложных и новых видов преступлений. И все же, следует констатировать, что до сих пор в системе криминалистической техники нет отдельного раздела, посвященного исследованию компьютерной техники, электронного денежного оборота, виртуальных следов преступлений. А потому данная проблема остается актуальной.

В криминалистической науке и практике виртуальные следы рассматриваются двояко, ввиду их специфичности. Их нельзя отнести ни к материальным, ни к идеальным. Учитывая, неподдельный интерес ученых и исследователей к указанной теме, на сегодняшний день имеется множество различных классификаций цифровых следов¹. Так, по форме носителя выделяют цифровые следы, расположенные на оптических, полупроводниковых и магнитных носителях; по способу доступа: доступ, к которым осуществляется локально или удаленно, размещенные в открытом доступе и защищенные следы; по месту хранения: во владении преступника (персональный компьютер, жесткий диск, мобильный телефон), на устройствах потерпевшего, свидетеля, сторонних лиц и цифровые следы, которые одновременно хранятся на устройствах всех указанных лиц и в сети Интернет. По типу устройства, на котором хранятся цифровые следы, выделяют стационарные и мобильные; по целевому предназначению: вредоносные программы и полезные программы (приложения с различными функциями, необходимые для осуществления операций или действий, помогающие в повседневной деятельности, в быту, работе и т.п.)².

Очевидно, что обнаружение, фиксация и изъятие цифровых следов преступления требует использования специальных знаний и технологий, разработка и совершенствование которых на протяжении последних нескольких лет представляет исключительно актуальное направление криминалистики. Таким образом, целесообразно говорить о введении самостоятельного подраздела криминалистической техники – криминалистического исследования электронных носителей информации и цифровых следов. Данный раздел должен обеспечить единообразие в работе соответствующих должностных лиц, сталкивающихся с рассматриваемой категорией объектов. Также мы считаем, что цифровым (виртуальным) следам следует отвести отдельное место в перечне всех изучаемых следов в криминалистике, а также определится с единой общепризнанной классификацией самих виртуальных следов.

В связи с развитием новых технологий необходимым становится развитие нового направления криминалистической идентификации, связанное с идентификацией технических средств по оставленным цифровым следам. Конечная цель такой идентификации – установление данных о лице, которое использовало интересующее техническое средство. Кроме того, определить соответствие информации, содержащейся

¹ Вехов В. Б. Понятие, виды и особенности фиксации электронных доказательств // Расследование преступлений: проблемы и пути их решения: сб. науч.-практ. трудов. М.: Академия Следственного комитета Российской Федерации, 2016. № 1. С. 156.

² Бахтеев Д. В. Криминалистическая классификация цифровой доказательственной информации: сборник статей Международной научно-практической конференции «Криминалистика в условиях развития информационного общества» (59-е ежегодные криминалистические чтения). М.: Академия управления МВД России, 2018. С. 46–47.

на различных электронных носителях, или наличие на электронном носителе информации с заданными характеристиками не представляется возможным с помощью традиционных видов криминалистической идентификации.

К сожалению, требования к объему настоящего исследования не позволяют перечислить все проблемы, связанные с развитием цифровой криминалистики. Например, сам термин «цифровая криминалистика», по нашему мнению, не считается устоявшимся. Не ясно, как соотносятся понятия электронные, виртуальные, цифровые следы. Нет четких методик по работе с некоторыми видами указанных следов. Имеющиеся практические рекомендации узконаправленны и требует частого обновления ввиду развития новой техники и возможностей сотовой сети и сети Интернет. Процесс расследования преступлений, способов обнаружения, изъятия и фиксации «электронных следов» – все это, однозначно требует введения инновационного подхода в криминалистической науке. На наш взгляд, развитие цифровой криминалистики как отдельного направления криминалистики, позволит решить указанные проблемы. Учитывая стремительные темпы научно-технического прогресса, совершенствовать и пополнять цифровую криминалистику необходимо незамедлительно и во взаимодействии ученых, специалистов и практических сотрудников.

Список литературы

1. Филиппова Е. Криптовалюту в России собираются узаконить в первой половине года // Парламентская газета. Экономика. [Электронный ресурс]. Дата обновления: 20.03.2018. Режим доступа: <https://www.pnp.ru/economics/kriptovalyutu-v-rossii-sobirayutsya-uzakonit-v-pervoy-polovine-goda.html>.
2. Бахтеев Д. В. Криминалистическая классификация цифровой доказательственной информации: сборник статей Международной научно-практической конференции «Криминалистика в условиях развития информационного общества» (59-е ежегодные криминалистические чтения). М.: Академия управления МВД России, 2018. С. 44-50.
3. Вехов В. Б. Понятие, виды и особенности фиксации электронных доказательств // Расследование преступлений: проблемы и пути их решения: сб. науч.-практ. трудов. М.: Академия Следственного комитета Российской Федерации, 2016. № 1.

Roman A. Deryugin

PhD in Law, Lecturer of the Department of Criminalistics
Ural Law Institute of the Ministry of Internal Affairs of Russia
(Russia, Yekaterinburg)
deryugin.r.a@mail.ru

Anastasia A. Zhizhileva

Cadet of the Faculty of Investigators Training
(Russia, Yekaterinburg)
zhizhileva74@mail.ru

PROSPECTS OF DEVELOPMENT OF DIGITAL CRIMINALISTICS IN THE CONDITIONS OF THE INFORMATION SOCIETY

Abstract: The article discusses trends in the development of digital forensics in the context of improving and expanding the capabilities of the Internet, mobile applications, in particular, instant messengers and the spread of cryptocurrencies. The authors investigate issues related to the use of a virtual (electronic) track in the process of investigating and investigating crimes.

Keywords: information technology, Internet, cryptocurrency, «fake» information, electronic traces, virtual traces, digital forensics.

Долинин Владимир Николаевич

Кандидат юридических наук, доцент, доцент кафедры криминалистики
Уральский государственный юридический университет
(г. Екатеринбург)
dvn1952@gmail.com

Кабитова Юлия Равилевна

студент Института прокуратуры
Уральский государственный юридический университет
(г. Екатеринбург)
juliaravil@yandex.ru

Елькина Полина Сергеевна

Студент Института прокуратуры
Уральский государственный юридический университет
(г. Екатеринбург)
polina_elkina_98@mail.ru

**ТЕХНОЛОГИИ СОБИРАНИЯ, ИССЛЕДОВАНИЯ И ИСПОЛЬЗОВАНИЯ
ЭЛЕКТРОННО-ЦИФРОВЫХ ДОКАЗАТЕЛЬСТВ**

Аннотация: В связи с информатизацией общества, появляются новые доказательства в уголовном процессе и в криминалистике в частности электронно-цифровые доказательства. В представленной статье рассматриваются понятия электронных доказательств, приводится их классификация различных ученых, юристов. Описание следственных действия: осмотр места происшествия, осмотр предметов, обыск, которые являются источником получения этих доказательств. Особое внимание уделяются описанию различных видов компьютерно-технической экспертизы и постановке вопросов эксперту.

Ключевые слова: электронно-цифровые доказательства, технологии, осмотр предметов, содержащих электронную информацию, обыск, выемка, компьютерно-техническая экспертиза, допрос.

В современном мире происходит глобализация и информатизация, совершенствуется информационное пространство, информационные технологии используются повсеместно, в том числе и при совершении преступлений. В следственной практике появились новые доказательства, а именно электронно-цифровые доказательства. Определение электронных доказательств отсутствует в уголовно-процессуальном кодексе Российской Федерации, но в науке приводятся различные определения. Так, Р. И. Оконенко в своей диссертационной работе дает определение «под «электронным доказательством» понимается электронный носитель информации, содержащий сведения о значимых обстоятельствах по конкретному уголовному делу и обладающий следующими юридически значимыми признаками: а) значительным объемом памяти; б) простотой передачи и копирования сведений с одного электронного носителя информации на другой; в) возможностью удаленного доступа к содержанию электронного

носителя и информационно-телекоммуникационным системам (в частности к сети Интернет); г) относительностью и неочевидностью содержания»¹.

Е. Р. Россинская определила, «цифровые следы определяются, как материальные невидимые следы, они зафиксированы на материальном носителе либо передаются по каналам связи посредством электронных сигналов»².

Представляет интерес суждения В. Ю. Ангibalова, который считает, что цифровые следы, отражаясь на материальном носителе фиксируют лишь образ, состоящий из цифровых значений параметров формальной математической модели наблюдаемого реального физического явления³. Т. Э. Кукарникова отмечает: «электронные доказательства-объект, несущий информацию, имеющий смысловое значение и существующий только в электронной среде»⁴. В. Б. Вехов утверждает, что «электронно-цифровой след – любая криминалистически значимая компьютерная информация, то есть сведения, находящиеся в электронно-цифровой форме, зафиксированное на материальном носителе»⁵. Аналогичное суждение высказывает и П. С. Пастухов⁶.

Данный вид доказательств не выделен в отдельную группу доказательств. Действующий уголовно-процессуальный кодекс относит данный вид доказательств к вещественным, если они обладают признаками, перечисленными в статье 81 УПК РФ, если не содержат таких признаков, то признаются иными документами в соответствии с статьей 84 УПК РФ. По нашему мнению, между данным видом доказательств и вещественными необходимо проводить разграничение. Вещественные доказательства – это предметы материального мира, а электронная информация только находится на материальном носителе, но он не отражает информацию, которая на нем записана, а доказательством является именно информация. В вещественном доказательстве информация содержится в своем естественном виде и преобразование для ее восприятия не нужно. Для восприятия электронной информации необходимо использование технического средства. С. В. Калитин в своем научном труде отграничивает электронные доказательства от вещественных, при этом он подчеркивает, что данные доказательства необходимо разделить на 2 самостоятельных группы как это делают в зарубежных странах: электронные и цифровые. «Электронная часть доказательств связана только с электронными приборами или сокращенно – электроникой – техникой, использующей для работы электроны, а именно – электричество»⁷. Цифровые доказательства – это информация, которая закодирована, с помощью двоичной системы. «Цифровой сигнал не меняется со временем. Меняется носитель»⁸.

Классификацию цифровых следов одним из первых предложил А. Ю. Семенов. Он выделил: 1) следы на жестком диске (винчестере), магнитной ленте («стримере»), оптическом диске (CD, DVD), на дискете (флоппи диске); 2) следы в оперативно запоминающих устройствах (ОЗУ), ЭВМ; 3) следы в ОЗУ периферийных устройств (например, лазерного принтера); 4) следы в ОЗУ компьютерных устройств связи и

¹ Оконенко Р. И. «Электронные доказательства» и проблемы обеспечения прав граждан на защиту тайны личной жизни в уголовном процессе: сравнительный анализ законодательства Соединенных Штатов Америки и Российской Федерации: дис. ... канд. юрид. наук. М., 2016.

² Россинская Е. Р., Шамаев Г. П. Новый раздел криминалистики: криминалистическое исследование компьютерных средств и систем // Электронный научный журнал. 2015. Т.6. № 1. с. 234-241.

³ Ангibalов В. Ю. Виртуальные следы в криминалистике и уголовном процессе. Воронеж, 2010. С. 14-15.

⁴ Кукарникова Т. Э. Электронный документ в уголовном процессе и криминалистике. Воронеж, 2008. С. 28-29.

⁵ Вехов В. Б. Криминалистическое учение о компьютерной информации и средствах ее обработки. Волгоград, 2008. С. 59.

⁶ Пастухов П. С. Электронное вещественное доказательство в уголовном судопроизводстве. 2015. С. 149-150.

⁷ Калитин С. В. Доказательства электронные и цифровые // Научно-методический электронный журнал «Концепт». 2014. Т. 20. С. 3586–3590.

⁸ Там же.

сетевых устройств; 5) следы в проводных, радио-оптических и других электромагнитных систем, и сетей связи¹.

По классификации А. Г. Волеводза следы делятся на локальные и сетевые. Д. Пашнев классифицировал следы в зависимости от механизма следообразования и выделил: 1) в системных областях файловой системы; 2) в файлах программ и данных (файлы документов и файлы настроек программ); 3) в кластерах физических носителей информации².

В классификации Л. Б. Красновой был использован аналогичный механизм следообразования и выделены виртуальные первичные-следствие непосредственного воздействия пользователя с использованием какой-либо информационной технологии, и вторичные – следствие воздействия технологических процессов без участия человека и вне его желания³.

Собирание доказательств представляет собой совокупность действий по обнаружению, фиксации, изъятию и сохранению различных доказательств⁴. Электронные доказательства, как и другие доказательства, собираются путём проведения следственных и иных процессуальных действий.

Осмотр места происшествия. Осмотр места происшествия, то есть действия по сбору доказательств. К осмотру места происшествия необходимо привлекать специалистов. Задача осмотра – это определение места нахождения всех компьютеров, входящих в систему или сеть. Выясняются способы их объединения (локальная сеть, прямое включение и т. д.); определяются способы связи компьютеров; определяются тип и модель компьютеров и др. Производство осмотра места происшествия обычно проводится в «помещениях, где находится несколько компьютерных устройств и работают достаточное количество людей и это сопряжено со значительными трудностями»⁵.

Осмотр предметов, содержащих электронную информацию. При осмотре предметов, являющихся носителями электронной информации, описание осуществляется при соблюдении следующих правил⁶ а) общий обзор ведётся от внешнего содержания к внутреннему и от индивидуальных признаков, свидетельствующих о связи с преступлением; б) детальный их осмотр во время изъятия не исключает их осмотра в качестве отдельного предмета; в) в осмотре участвуют эксперт-криминалист и квалифицированный специалист в сфере информации.

При производстве осмотра описание носителя электронной информации осуществляется по следующему плану:

1. Описание носителя электронной информации: а) внешний осмотр, расположение рабочих механизмов осматриваемого предмета и внешних устройств относительно друг друга на момент осмотра и в пространстве; б) устанавливается какого типа, марки, конфигурации, цвета основной осматриваемый предмет и каждого комплектующего устройства; в) состояние предмета на момент начала осмотра; г) информация, содержащаяся на экране; д) техническое состояние (внешнее состояние корпусов, комплектность, работоспособность устройств); е) описание источника электрического снабжения, его характеристики и техническое состояние; ж) подробное описание изменений, которые не предусмотрены общими стандартами для таких типов технических средств;

¹ Семенов А. Ю. Некоторые аспекты выявления, изъятия и исследования следов, возникающих при совершении преступлений в сфере компьютерной информации // Сибирский юридический вестник. 2004. № 1.

² Пашнев Д. Понятия и классификация следов исследования компьютерных технологий [Электронный ресурс]. 2004. Режим доступа: <http://www.crime-research.ru/articles/Pashnev2/2> (дата обращения: 18.05.2019).

³ Краснова Л. Б. Компьютерные объекты в уголовном процессе и криминалистике. Воронеж, 2005. С.17.

⁴ Драпкин Л. Я., Карагодин В. Н. Криминалистика. М, 2011.

⁵ Криминалистика: учебник / под ред. Т.В. Аверьяновой. М, 2013. С.908.

⁶ Зуев С. В. Осмотр и изъятие электронных носителей информации при проведении следственных действий и оперативно-розыскных мероприятий // Законность. 2018. № 4. С. 58-60.

2. Описание и сбор информации в электронной форме: а) проверка наличия программных средств защиты информации и возможности ее отправления по техническим каналам; в) результаты тестирования специалистами информации для выявления скрытой информации, а также ранее уничтоженной; г) содержание информации, которая хранится в носителе информации и ее внешних устройствах; д) распечатывание информации на бумаге печатными средствами, характеристика которых описывается в протоколе; е) повторная упаковка с надлежащей последовательностью носителей электронной информации; упаковка бумажных носителей с полученной информацией. Затем должна быть произведена фиксация обстановки и обстоятельств, при которых обнаружены электронные объекты путем составления протокола осмотра и фото-и видеосъемки.

Обзор носителей компьютерной информации (дисков, флэш-карт и т.п.) имеет следующие особенности: а) в начале обзора следует описать индивидуальные признаки защитных механизмов носителя электронной информации от изменения или несанкционированного копирования; б) перед тем, как исследовать информацию, необходимо обязательно создать резервную копию данной информации; в) на следующем этапе осмотра фиксируется общий объем носителя компьютерной информации; формат разметки; объем памяти, свободный от записи информации и т. д; количество и перечень файлов, программ; г) необходимо техническим способом защитить физический накопитель от записи или стирания с него информации.

В следственной практике часто проводится осмотр сотовых телефонов (смартфонов), которые осматриваются по правилам осмотра любого предмета с присущими особенностями¹.

Осмотр смартфона, полагаем, можно разделить на три этапа:

1. Подготовительный этап – включает в себя выбор места, подготовку освещения, приглашение понятых, приглашение специалистов сотовой связи для консультации; изучение специальной справочной литературы (определение характеристик смартфона); подготовку измерительных приспособлений, увеличительных приборов (лупа с подсветкой) и другие необходимые действия.

2. Основной этап включает 3 стадии:

1) Внешний осмотр. На данной стадии необходимо изучить и зафиксировать общие признаки: тип и состояние смартфона, указать его размеры, марку, модель, форму цвет, наличие объективов тыльной и лицевой фото/видеокамеры, фирменных наименований, логотипа, обозначений; количество и расположение сенсорных клавиш; разъемов Mini (Micro) USB зарядного устройства, стереонаушников; наличие отверстия для динамика, микрофона, внешней освещенности. Особенно важно зафиксировать особые приметы наружного строения-сколы, царапины, потертости, отсутствие должных элементов; наличие дополнительных атрибутов и защитных элементов корпуса смартфона-чехла, полимерных наклеек, графических ставок, надписей, инкрустацией драгоценными металлами. В ходе внешнего осмотра нужно провести детальную фотосъемку внешней, оборотной, боковых, панелей смартфона.

2) Внутренний осмотр. На данной стадии проводится осмотр конструкции телефона по частям задней крышки смартфона и (или) аккумуляторной батареей, флэш-карты, SIM-карты. При осмотре аккумуляторной батареи в протоколе следует указать ее идентификационный номер, тип, марку, модель, мощность и т.д. Также в протоколе нужно указать цвет и материал, из которого батарея изготовлена. При осмотре флэш-карты (Mini SD) необходимо обратить пристальное внимание на ее идентификационный номер, объем, цвет, материал корпуса. SIM-карта, обнаруженная в смартфоне, осматривается аналогичным образом типовая ситуация, когда на SIM-карте указан логотип оператора сотовой связи, поэтому описание его также обязательно в протоколе.

¹ Драпкин Л. Я., Долинин В. Н. Тактика следственных действий. Учебно- практическое пособие. Издание третье, дополненное. Екатеринбург: Издательский дом УрГЮУ, 2015. С. 25.

В ходе внутреннего осмотра проводится детальная фотосъемка внешней и обратной стороны батареи, флэш-карты, SIM-карты, а также тыльной стороны корпуса смартфона (без задней крышки), чтобы на снимке отразить IMEI-номер аппарата.

3) Осмотр информационного содержания. Осмотр информационного содержания включает в себя изучение и фиксацию сведений, которые содержатся в памяти смартфона, флэш-карты, SIM-карты. Если смартфон удалось включить и он получил доступ к сведениям, которые в смартфоне содержатся, в протоколе в хронологическом порядке нужно зафиксировать все производимые в дальнейшем манипуляции.

3. Заключительный этап состоит в составлении протокола осмотра предметов (документов).

Протокол осмотра предметов включает следующие структурные элементы: вводную и описательную части.

Во вводной части указываются число, месяц, год, место производства этого следственного действия, время его начала и окончания, сведения об участниках, точное место и условия проведения (адрес, погода, освещенность), использование технических средств, перечень изымаемых предметов.

В описательной части фиксируются все действия следователя в той последовательности, в которой они производились. К протоколу могут прилагаться графические изображения (фототаблицы, планы, схемы).

В следственной практике и среди ученых-криминалистов возникают споры по поводу того, в каком состоянии должен изыматься смартфон. Г. В. Семенов утверждает, что «его не следует отключать, т.к. при последующем включении могут потребоваться коды блокировки, необходимые для работы телефона и соответственно исследования его информационного содержимого»¹. Защитные коды могут обеспечить как полную блокировку аппарата, так и ограничивать доступ к использованию некоторых функций.

Поэтому на наш взгляд, изъятие смартфона необходимо проводить все же во включенном состоянии. Иными словами, следователь при изъятии, выключив смартфон, столкнется с проблемой получения информации, содержащейся в памяти телефона, и придется обращаться за помощью к специалисту, что потребует времени (от нескольких часов до недели), что повлечет за собой утерю оперативности и своевременного расследования преступления.

Обыск и выемка при расследовании преступлений. Порядок и основания проведения обыска и выемки содержатся в ст.ст. 182 и 183 УПК РФ соответственно. Так, согласно ст. 182 УПК РФ, основанием для осуществления обыска является наличие достаточных данных полагать, что в каком-либо месте или у какого-либо лица могут находиться орудия, оборудование или иные средства совершения преступления, предметы, документы и ценности, которые могут иметь значение для уголовного дела. И в соответствии со ст. 183 УПК РФ определённые предметы и документы, имеющие значение для уголовного дела, при необходимости могут быть изъяты.

Цель проведения обыска (выемки) цифровой информации - обнаружение, фиксация и изъятие компьютерной техники, на которой имеются следы цифровой информации, имеющей значение для уголовного дела. Его результаты зависят от подготовки к предстоящему производству. Проанализировав труды различных ученых, касающейся данной темы, выявлены такие особенности²:

На подготовительном этапе обыска (выемки) следователю необходимо:

1. Проанализировать имеющиеся сведения о преступлении и определить, каким может быть содержание электронной информации,; установить, на каких носителях (например, жёсткий диск, флэш-карта) может содержаться такая информация; какие

¹ Варданян А. В. Обыск и проблемы участия понятых в его производстве // Общество и право. 2008. № 2.

² Дворкин А. И. Осмотр места происшествия: практическое пособие. М.: Юрист: Библиотека следователя, 2001.

технические средства (например, телефон, планшет и т.п.), относящаяся к преступлению, могут быть на месте обыска.

2. Сбор информации о месте обыска (выемки). Необходимо получить данные о местонахождении этого места; характеристика строения; планировка помещений; этажности; количестве комнат, имеется ли работающий модем; сеть Wi-Fi; соединена ли компьютерная техника между собой локальной сетью; нахождение системы электрического питания.

3. Изучение личности обыскиваемого и проживающих (находящихся) с ним лиц. Данные о профессии и месте работы, образа жизни и связей, навыках и умениях работы с техническими средствами, профессиональных знаниях

4. Подготовка транспорта и технических средств, к ним относятся антивирусные программы, мобильный комплекс по сбору и анализу цифровых данных «UFED» и т.д.), согласованных со специалистом.

5. Подготовка следственно-оперативной группы. Необходимо, чтобы при обыске (выемке) обязательно участвовали специалист и понятые. Понятые должны обладать навыками пользования компьютером для того, чтобы понимать суть производимых действий.

Затем следственно-оперативная группа проникает на место обыска, устанавливает личность обыскиваемых, объявляет, распределяет обязанности между участниками следственного действия. После этого следователь приступает к производству обыска (выемки).

После прибытия на место обыска и выемки и проникновения на объект, войдя в помещение, следователь должен представиться и о предъявить постановление о производстве обыска, затем предложить добровольно выдать искомые предметы. В случае, если обыскиваемые лица откажутся, то следователь запрещает лицам доступ к компьютерной технике (компьютер, ноутбук, смартфон, планшетный компьютер, плеер и прочее).

Следующий этап: поисковый. Он делится на обзорную и детальную стадии.

На обзорной стадии следователь должен:

1. Осуществить визуальный осмотр всего помещения. Следственно-оперативной группе необходимо обращать внимание на технические средства и портативные устройства, находящиеся в помещении, так как цифровая информация будет обнаружена в электронном носителе. Иногда, преступники, являющиеся профессионалами в сфере информатизации (программист, системный администратор и т.д.) могут скрыть искомую информацию в различные предметы (например, бижутерия).

2. Необходимо установить количество компьютеров в помещении. Имеется ли объединение нескольких компьютеров в одну локальную сеть, и если имеется, то определить базовый компьютер и обыск начать с него.

3. Следователь вместе со специалистом проверяют, имеются ли на материальном носителе защита информации, вирусные программы, удаленный доступ. Так как их наличие может привести к полному уничтожению искомой информации или ее повреждению. Например, если на носителе имеется удаленный доступ, то преступное лицо может без доступа к нему совершить различные действия: удалить информацию, заблокировать, изменить и т.д.

4. Специалист, осматривая компьютер должен установить вид операционной системы; перечень программ и выполняемых с ними действий и т.д.

На детальной стадии процессуального действия следователь должен:

5. В том случае, если нет риска, что цифровая информация может быть уничтожена или повреждена, то следователь вместе со специалистом должны начать поиск необходимой информации. Проведение поиска основывается на сведениях о цифровой информации, предположениях, где она может быть обнаружена. При нахождении искомой информации, должно быть указано точное расположение места ее нахождения.

По окончании осмотра, компьютер должен быть выключен, упакован и изъят.

Следует подчеркнуть, что обязательно должен присутствовать специалист, требование, которое установлено законодателем, обеспечивает соблюдение законных прав и интересов владельцев и обладателей информации. В случаях, когда заявлено ходатайство законного владельца или лицом, обладающим информацией специалистом, участвующим в следственном действии, в присутствии понятых с изымаемых электронных носителей информации осуществляется копирование информации. Копирование информации на другие электронные носители информации, которые предоставляются законным владельцем изымаемых электронных носителей информации или обладателем содержащейся на них информации. Электронные носители информации, содержащие скопированную информацию, передаются законному владельцу изымаемых электронных носителей информации или обладателю содержащейся на них информации. Об осуществлении копирования информации и о передаче электронных носителей информации, содержащих скопированную информацию, законному владельцу изымаемых электронных носителей информации или обладателю содержащейся на них информации в протоколе следственного действия делается запись. Следовательно в ходе производства следственного действия вправе осуществить копирование информации, содержащейся на электронном носителе информации.

6. При окончании обыска (выемки) все обнаруженные технические средства, которые содержат цифровую информацию, имеющую значение для уголовного дела перед изъятием правильно упаковываются и опечатываются. Затем составляется протокол следственного действия и описи к нему.

После изъятия предметов, они направляются на исследование.

При расследовании преступлений в сфере компьютерной информации применяется специфический род экспертиз, относящийся к категории инженерно-технических экспертиз – судебная компьютерно-техническая экспертиза. В рамках этого рода экспертиз в 1996 году Е. Р. Россинская выделила два вида¹:

– техническая экспертиза компьютеров и их комплектующих в целях изучения конструктивных особенностей и состояния компьютера, его периферийных устройств, магнитных носителей и пр., также причин возникновения сбоев в работе вышеуказанного оборудования;

– экспертизу программного обеспечения и данных, которая осуществляется для изучения информации, хранящейся в компьютере и на магнитных носителях.

У данных экспертиз различаются объекты исследования. Так при технической экспертизе объектами исследования являются материальные носители информации о факте или событии уголовного дела. Ими могут быть персональные компьютеры, флэш-карты, магнитные и лазерные диски, различные микросхемы и др. устройства. А при экспертизе программного обеспечения и данных объектами уже являются, например, файлы, созданные с помощью ЭВМ и других технических средств - с расширениями текстовых форматов, графических форматов, база данных, электронная таблица, мультимедиа, запись пластиковой карты и др.

Позднее Е. Р. Россинская расширила классификацию компьютерно-технической экспертизы. Было выделено четыре вида²:

- 1) аппаратно-компьютерная экспертиза;
- 2) программно-компьютерная экспертиза;
- 3) информационно-компьютерная экспертиза (данных);
- 4) компьютерно-сетевая экспертиза.

¹ Россинская Е. Р. Компьютерно-техническая экспертиза // Информационный бюллетень № 1. М.: Академия МВД РФ, кафедра КОД ОВД, 1996; Россинская Е. Р. Судебная экспертиза в уголовном, гражданском и арбитражном процессе. М.: Право и закон, 1996.

² Россинская Е. Р., Галяшина Е. И. Настольная книга судьи: судебная экспертиза. Москва: Проспект, 2010. С. 258.

Следователь должен поставить перед экспертом конкретные вопросы, на которые экспертиза должна дать ответ. От правильности этих вопросов, от степени охвата ими существенных обстоятельств дела и четкости их формулировки в значительной степени зависит результат двусмысленность, а кроме того, иметь строгую последовательность. Постановка вопросов эксперту зависит от вида компьютерно-технической экспертизы.

1. Вопросы при назначении аппаратно-компьютерной экспертизы:

- «Относится ли представленное устройство к аппаратным компьютерным средствам?»
- «К какому типу (марке, модели) относится аппаратное средство?»
- «Каковы его технические характеристики и параметры?»
- «Каково функциональное предназначение аппаратного средства?»
- «Какова роль и функциональные возможности данного аппаратного средства в конкретной компьютерной системе?»
- «Относится ли данное аппаратное средство к представленной компьютерной системе?»
- «Используется ли данное аппаратное средство для решения конкретно функциональной задачи?»
- «Какое первоначальное состояние (конфигурацию, характеристики) имело аппаратное средство?»
- «Каково фактическое состояние (исправен, неисправен) представленного аппаратного средства?»
- «Имеются ли в нем отклонения от типовых (нормальных) параметров, в том числе и физические дефекты?»
- «Какие эксплуатационные режимы установлены на данном аппаратном средстве?»

2. Вопросы при назначении программно-компьютерной экспертизе:

- «Какова общая характеристика представленного программного обеспечения, из каких компонент (программных средств) оно состоит?»
- «Какую классификацию имеют конкретные программные средства (системные или прикладные) представленного программного обеспечения?»
- «Каково наименование, тип, версия, вид представления (явный, скрытый, удаленный) программного средства?»
- «Каковы реквизиты разработчика и владельца данного программного средства?»
- «Каков состав соответствующих файлов программного обеспечения, каковы их параметры (объемы, даты создания, атрибуты)?»
- «Какое общее функциональное предназначение имеет программное средство?»
- «Имеются ли на носителях информации программные средства для реализации определенной функциональной задачи?»
- «Какие требования предъявляет данное программное средство к аппаратным средствам компьютерной системы?»
- «Какова совместимость конкретного программного средства с программным и аппаратным обеспечением компьютерной системы?»
- «Используется ли данное программное средство для решения определенной функциональной задачи?»
- «Каково фактическое состояние программного средства, его работоспособность по реализации отдельных (конкретных) функций?»

3. Вопросы при назначении информационно-компьютерной экспертизы:

- «Как отформатирован носитель информации и в каком виде на него записаны данные?»

- «Каковы характеристики физического размещения данных на носителе информации?»
 - «Каковы характеристики логического размещения данных на носителе информации?»
 - «Какие свойства, характеристики и параметры (объемы, даты создания-изменения, атрибуты и др.) имеют данные на носителе информации?»
 - «Какого вида (явный, скрытый, удаленный, архив) информация имеется на носителе?»
 - «К какому типу относятся выявленные (определенные) данные (текстовые, графические, база данных, электронная таблица, мультимедиа, запись пластиковой карты, данные ПЗУ и др.) и какими программными средствами они обеспечиваются?»
 - «Каким образом организован доступ (свободный, ограниченный и проч.) к данным на носителе информации и каковы его характеристики?»
 - «Какие свойства, характеристики имеют выявленные средства защиты данных и какие пути ее преодоления возможны?»
 - «Какие признаки преодоления защиты (либо попыток несанкционированного доступа) имеются на носителе информации?»
4. Вопросы при назначении компьютерно-сетевой экспертизы:
- «Имеются ли признаки работы данного компьютерного средства в сети Интернет?»
 - «Какие аппаратные средства использовались для подключения к Интернету?»
 - «Имеются ли заготовленные соединения с узлом сети Интернет и каковы их свойства (номера телефонов провайдера, имена и пароли пользователя, даты создания)?»
 - «Каково содержание установок программы удаленного доступа к сети Интернет и протоколов соединений?»
 - «Какие имеются адреса Интернета, по которым осуществлялся доступ с данного компьютерного средства?»
 - «Имеется ли какая-либо информация о проведении электронных платежей и использовании кодов кредитных карт?»
 - «Имеются ли почтовые сообщения, полученные (а также отправленные) по электронной почте?»
 - «Имеются ли сообщения, полученные (отправленные) посредством использования программ персональной связи через Интернет и каково их содержание?»

Постановка вопросов эксперту при производстве компьютерно-технической экспертизы различного вида является одной из самых важных составляющих данного следственного действия, поскольку от правильно поставленных вопросов, их полноты зависит доказательственное значение экспертизы, необходимой для установления состава преступления, совершаемого при помощи компьютерных технологий.

По окончании экспертизы эксперт составляет заключение, которое используется в дальнейшем следователем при допросе как доказательство. Использование в расследовании электронно-цифровых доказательств применяется в процессе допроса свидетелей, подозреваемых, обвиняемых. При предъявлении электронных и цифровых доказательств используются такие же приемы, как и для вещественных. Первый прием связан с системным подходом, при котором взаимосвязанные доказательства предъявляются параллельно, либо последовательно. Так же одним из часто используемых приемов применяемый в практике – предъявление доказательств от менее слабых к более сильным. Возможно и использование сразу решающего доказательства.

При допросах свидетелей и потерпевших необходимо выяснить:

- Назначение и функции компьютерной системы; кто имел доступ к ней и в помещения, где располагалась компьютерная техника;

- Не появлялись ли там посторонние лица; какие средства защиты использовались; кто санкционировал доступ к информации (если она была закрытой) и кто реально был допущен;

- Какой вред (имущественный, неимущественный) причинен преступлением и имеются ли способы его уменьшить

При допросах подозреваемых или обвиняемых необходимо учитывать данные криминалистической характеристики о личности предполагаемого преступника. При первоначальном допросе, побуждая лицо к деятельному раскаянию, необходимо выяснить:

- Какие изменения в работу компьютерных систем были внесены
- Какие вирусы использовались

Решение вопроса о привлечении специалиста к участию в допросе остается на усмотрение следователя. В случае его участия при производстве допроса следователь имеет возможность получить от специалиста исчерпывающую информацию о механизме преступления и его отдельных элементах, что может оказать воздействие на допрашиваемое лицо и получить правдивые показания.

Список литературы

1. Агibalов В. Ю. Виртуальные следы в криминалистике и уголовном процессе. Воронеж, 2010.
2. Варданян А. В. Обыск и проблемы участия понятых в его производстве // Общество и право. 2008. № 2.
3. Вехов В. Б. Криминалистическое учение о компьютерной информации и средствах ее обработки. Волгоград, 2008.
4. Винберг А. И. Криминалистика.
5. Дворкин А. И. Осмотр места происшествия: практическое пособие. М.: Юрист: Библиотека следователя, 2001.
6. Драпкин Л. Я., Долинин В. Н. Тактика следственных действий. Учебно-практическое пособие. Издание третье, дополненное. Екатеринбург: Издательский дом УрГЮУ, 2015.
7. Ермакова Е. С., Джумангалиева Д. М. Электронные доказательства как новое направление в практике расследования преступлений // Молодой ученый. 2018. № 23.
8. Зигура Н. А. Компьютерная информация как вид доказательств в уголовном процессе России.
9. Зуев С. В. Осмотр и изъятие электронных носителей информации при проведении следственных действий и оперативно-розыскных мероприятий // Законность. 2018. № 4.
10. Калитин С. В. Доказательства электронные и цифровые // Научно-методический электронный журнал «Концепт». 2014. Т. 20.
11. Криминалистика: учебник / под ред. Т.В. Аверьяновой. М, 2013.
12. Кукарникова Т. Э. Электронный документ в уголовном процессе и криминалистике. Воронеж, 2008.
13. Оконенко Р. И. «Электронные доказательства» и проблемы обеспечения прав граждан на защиту тайны личной жизни в уголовном процессе: сравнительный анализ законодательства Соединенных Штатов Америки и Российской Федерации: дис. ... канд. юрид. наук. М., 2016.
14. Пастухов П. С. Электронное вещественное доказательство в уголовном судопроизводстве. 2015.
15. Пашнев Д. Понятия и классификация следов исследования компьютерных технологий [Электронный ресурс]. 2004. Режим доступа: <http://www.crime-research.ru/articles/Pashnev2/2>

16. Россинская Е. Р. Компьютерно-техническая экспертиза // Информационный бюллетень № 1. М.: Академия МВД РФ, кафедра КОД ОВД, 1996.
17. Россинская Е. Р., Галяшина Е. И. Настольная книга судьи: судебная экспертиза. Москва: Проспект, 2010.
18. Россинская Е. Р., Шамаев Г. П. Новый раздел криминалистики: криминалистическое исследование компьютерных средств и систем // Электронный научный журнал. 2015. Т.6. № 1.
19. Семенов А. Ю. Некоторые аспекты выявления, изъятия и исследования следов, возникающих при совершении преступлений в сфере компьютерной информации // Сибирский юридический вестник. 2004. № 1.
20. Чернышов В. Н., Лоскутова Е. С. Проблемы собирания и использования цифровых доказательств // Социально-экономические явления и процессы. 2017. Т. 12. № 5.

Vladimir N. Dolinin

PhD in Law, Associate Professor, Associate Professor of the Department of Criminalistics
Ural State Law University
(Russia, Yekaterinburg)
dvn1952@gmail.com

Julia R. Kabitova

Student of Institute of Prosecutor's Office,
Ural State Law University
(Russia, Yekaterinburg)
juliaravil@yandex.ru

Polina S. Elkina

Student of Institute of Prosecutor's Office,
Ural State Law University
(Russia, Yekaterinburg)
polina_elkina_98@mail.ru

**TECHNOLOGIES FOR COLLECTION, EXAMINATION AND USE OF ELECTRONIC
DIGITAL EVIDENCE**

Abstract: In connection with the informatization of society, there are new evidence in the criminal process and in criminology in particular electronic-digital evidence. The article deals with the concepts of electronic evidence, their classification of various scientists and lawyers. Description of investigative actions: inspection of the scene, inspection of objects, search, which are the source of this evidence. Particular attention is paid to the description of various types of computer-technical expertise and questions to the expert.

Keywords: digital evidence, technologies of examination of objects containing electronic information, search, seizure, computer-technical expertise, interrogation.

Желватых Александр Александрович

Партнер

Центр правовых услуг «Регус»

(г. Екатеринбург)

regus10@mail.ru

ОПАСНОСТИ КРИПТОВАЛЮТНЫХ «ПИРАМИД»: ОПЫТ СУДЕБНОЙ ПРАКТИКИ

Аннотация. На волне роста популярности криптовалют появляются сомнительные финансовые организации, члены которых под видом игры на курсе криптовалют занимаются сбором денег с населения. Люди отдают накопленное и влезают в долги. К сожалению, защитить их права в суде бывает нелегко из-за того, что граждане вступают в такие «клубы» добровольно. В статье приведены некоторые примеры из судебной практики.

Ключевые слова: криптовалюта, биткойн, пирамида, суд, практика.

На волне роста популярности криптовалют многие люди стали интересоваться способами заработка при помощи сделок с криптовалютой. Причем варианты заработка условно можно поделить на два вида: честные и сомнительные. Честные – это погружение в техническую часть вопроса, изготовление и продажа ферм для т.н. «майнинга», сам майнинг, купли-продажа криптовалюты. Сомнительные – для любителей быстрого заработка «здесь и сейчас» – «криптовалютные клубы», рассказывающие своим вкладчикам и желающим ими стать про «радости» доверительного управления биткойном. Такие клубы привлекают доверчивых людей фотографиями в социальных сетях, на которых улыбочивые «бизнесмены» изображены на фоне дорогих машин, яхт, постоянно проводящими свой досуг на фешенебельных курортах.

К сожалению, взыскание денег в судебном порядке для обманутых вкладчиков таких «клубов» может быть затруднительно.

20.02.2017 Верховный Суд Республики Башкортостан вынес апелляционное определение по делу № 33-3487/2017,¹ оставив решение Нефтекамского городского суд Республики Башкортостан в силе. Истец просила взыскать с ответчика сумму неосновательного обогащения, ссылаясь на ошибочный перевод денежных средств. Однако суды первой и апелляционной инстанции указали на то, что материалами дела доказано обоснованность перевода в целях приобретения ответчиком электронной валюты «E-dinar». Денежные средства за покупку виртуальной валюты истец произвела добровольно. Суд признает, что осознанный перевод денег в целях приобретения криптовалюты не может являться основанием для возврата денежных средств, как неосновательного обогащения.

Аналогичной позиции придерживается Ульяновский областной суд в апелляционном определении от 31.07.2018 по делу № 33-3142/2018², в котором отменяет решение Ленинского районного суда города Ульяновска от 13.04.2018 и отказывает в удовлетворении исковых требований о взыскании неосновательного обогащения в сумме денег, переведенных истцами в целях участия в интернет-проекте Totem Capital. При этом

¹ Апелляционное определение Верховного Суда Республики Башкортостан от 20.02.2017 по делу № 33-3487/2017. Режим доступа: https://vs--bkr.sudrf.ru/modules.php?name=sud_delo&srv_num=1&name_op=doc&number=10851352&delo_id=5&new=5&text_number=1 (дата обращения: 18.05.2019).

² Апелляционное определение Ульяновского областного суда от 31.07.2018 по делу № 33-3142/2018. Режим доступа: http://uloblsud.ru/index.php?option=com_content&task=view&id=192&Itemid=63&idCard=74924 (дата обращения: 18.05.2019).

суд апелляционной инстанции указывает, что поскольку в Российской Федерации отсутствует какая-либо правовая база для регулирования платежей, осуществляемых в «виртуальной валюте», а также отсутствует какое-либо правовое регулирование торговых интернет-площадок, все операции с «виртуальной валютой» (криптовалютой) производятся их владельцами на свой страх и риск. Истцы, согласившись с условиями предоставления интернет-сайтом Totem Capital услуг обмена электронных валют, приняли на себя риск несения любой финансовой потери или ущерба.

Решением суда от 22.03.2019 Миасский городской суд Челябинской области¹ отказал во взыскании более чем одного миллиона рублей гражданке, поддавшейся на уговоры «агитатора» платформы «Альфа Кэш» и перечислившей ему деньги, поскольку признал приобретение криптовалюты для дальнейшего вложения в «криптоклуб» приобретением товара. При этом судья при вынесении решения посоветовал стороне Истца подать апелляционную жалобу в Челябинский областной суд, поскольку это первое подобное дело в регионе, и по такой категории дел не сформирована судебная практика.

На настоящий момент апелляционная жалоба по данному делу подана. В обоснование правовой позиции указано, в том числе, определение Верховного Суда Российской Федерации от 20.03.2018 № 66-КГ18-3,² согласно которому в схожей ситуации (истец перевела ответчику денежные средства в целях участия в проекте «Меркурий – взаимный фонд») было отменено апелляционное определение судебной коллегии по гражданским делам Иркутского областного суда от 29.03.2017, дело направлено на новое рассмотрение в суд апелляционной инстанции. Впоследствии апелляционным определением Иркутского областного суда от 07.05.2018 по делу № 33-3640/2018³ иски о взыскании неосновательного обогащения были удовлетворены.

Однако гарантировать, что суд апелляционной инстанции удовлетворит жалобу по аналогии с указанным делом нельзя, ведь в ситуации с проектом «Меркурий – взаимный фонд» истец не приобретал никакой криптовалюты.

Указанная практика судов общей юрисдикции сводится к тому, что судебные инстанции на данный момент не утруждают себя изучением технической стороны и правовой природы криптовалюты, а по сути признают криптовалютой любые «виртуальные деньги», ссылаясь на условия предоставления услуг обмена электронных валют с интернет-сайтов. Обратите внимание, что в судебных актах идет речь, в том числе, не об общеизвестных биткойнах, а о неких «интернет-проектах». Должен отметить, что такая судебная практика вызывает беспокойство, поскольку может формировать благоприятные условия для функционирования различных МММ-образных «клубов», созданных организаторами для сбора денег с населения под видом вложения в криптовалюту.

Кроме того, как видно из примера с Миасским городским судом Челябинской области, суды первой инстанции опасаются принимать решения без вышестоящей практики.

Aleksandr A. Zhelvatykh

Partner

Center of Legal Services «Regus»
(Russia, Yekaterinburg)

¹ Решение Миасского городского суда Челябинской области от 22.03.2019 по делу № 2-472/2019 .

² Определение Судебной коллегии по гражданским делам Верховного Суда Российской Федерации от 20.03.2018 № 66-КГ18-3. Режим доступа: <https://legalacts.ru/sud/opredelenie-verkhovnogo-suda-rf-ot-20032018-n-66-kg18-3/> (дата обращения: 18.05.2019).

³ Апелляционное определение Иркутского областного суда от 07.05.2018 по делу № 33-3640/2018. Режим доступа: https://oblsud--irk.sudrf.ru/modules.php?name=sud_delo&srv_num=1&name_op=doc&number=18747471&delo_id=5&new=5&text_number=1 (дата обращения: 18.05.2019).

**DANGER OF CRYPTOCURRENCY «PYRAMIDS»:
EXPERIENCE OF THE ARBITRAGE PRACTICE**

Abstract: On the wake of the growing popularity of the cryptocurrency dubious financial institutions appear whose members, under the guise of playing on a cryptocurrency course, collect money from the public. People give up accumulated money and go into debt. Unfortunately, it's not easy to protect their rights in courts due to the fact that citizens join such «clubs» voluntarily. The article contains some examples from the arbitrage practice.

Keywords: Cryptocurrency, bitcoin, pyramid, court, practice.

Зимин Владимир Владимирович

Помощник Головинского межрайонного прокурора г. Москвы,
аспирант Университета Прокуратуры Российской Федерации
(г. Москва)

Nivolkovis@gmail.com

НАУЧНО-ТЕХНИЧЕСКИЕ ДОСТИЖЕНИЯ И ПРЕСТУПЛЕНИЯ БУДУЩЕГО: ВОПРОСЫ КРИМИНОЛОГИЧЕСКОГО ПРОГНОЗИРОВАНИЯ И УПРЕЖДАЮЩЕЙ КРИМИНАЛИЗАЦИИ

Аннотация: В докладе утверждается необходимость уголовно-правового реагирования на преступления, связанные с искусственным интеллектом (ИИ), киберпреступлениями. Императивы защиты персональных данных, искусственного интеллекта и прав человека в условиях технологической конвергенции требуют новых методов отслеживания при помощи дронов и автоматического управления средствами передвижения. Предлагается создание на постоянной основе под эгидой ООН института, способного отслеживать не только возможное утилизацию самых недавних научно-технических разработок в целях анти-криминала, но и возможное предупреждение криминальности на основе прогнозирования событий.

Ключевые слова: ООН, ИИ, беспилотники, роботы, двойная наказуемость, дорожная карта, электронные доказательства, беспилотные автомобили.

27-29 ноября 2018 г. в г. Страсбурге (Франция) состоялось 75-е заседание Европейского комитета по проблемам преступности (далее – ЕКПП, Комитет), действующего в рамках Совета Европы – международной межправительственной организации, объединяющей почти все (47) европейских государств (кроме, Беларуси).

Сессия Комитета впервые прошла в экспериментальном режиме: один день был посвящен специальной тематической дискуссии, которая была сфокусирована на возможных мерах уголовно-правового реагирования на преступления, связанные с использованием «искусственного интеллекта». При этом была выбрана обозначившаяся во многих странах, в т. ч. в России, проблема определения ответственности, включая уголовную, в случаях инцидентов с участием «беспилотных автомобилей» (осуществляющих движение полностью или частично без управления водителем)¹.

Задействовав солидный потенциал приглашенных экспертов (в частности, из Австрии, Великобритании, Германии, Норвегии, США, Франции, Швейцарии), ЕКПП сделал первый шаг на пути изучения соответствующих этических и юридических аспектов с перспективой выхода на возможную рекомендацию Комитета министров Совета Европы или конвенцию Совета Европы, которые будут востребованы уже в ближайшем будущем.

Первоначальный анализ позволил обозначить ряд основных проблемных вопросов.

В настоящее время не существует общепризнанного (хотя бы на европейском уровне) определения «искусственного интеллекта» (ИИ) и каких-либо международных стандартов по его безопасному использованию. Имеющиеся в рамках Совета Европы смежные инструменты (например, т.н. Будапештская конвенция – Конвенция о киберпреступности (2001 г.), Конвенция о защите физических лиц при

¹ См., например: Штаге Д. Автоматизированное вождение и спорные ситуации // Уголовное право: стратегия развития в XXI веке: материалы XVI Международной научно-практической конференции. Москва: РГ-Пресс, 2019. С. 3-7; Баранчикова М. В. Проблемы квалификации дорожно-транспортных преступлений, совершенных с участием беспилотных транспортных средств // Там же. С. 8-12; Коробеев А. И., Чучаев А. И. Вред, причиненный роботомобилем: уголовно-правовые проблемы // Там же. С. 63-70.

автоматизированной обработке персональных данных (1981 г.), документы Парламентской ассамблеи Совета Европы, в частности, ее рекомендации 2069 (2015) «Дроны и целенаправленные убийства: необходимость соблюдения прав человека и международного права» и 2102 (2017) «Технологическая конвергенция, искусственный интеллект и права человека») пока не позволяют говорить о наличии и применении единой терминологии¹.

Нет ясного понимания и в вопросе о том, кто должен нести ответственность (уголовную и/или гражданско-правовую) в тех случаях, когда инцидент с участием «беспилотного автомобиля» приводит к нанесению вреда человеку или его смерти (водитель, оператор, производитель, разработчик программного обеспечения), какая может быть ответственность соответствующих компаний, а также в отношении санкций, которые могут применяться к физическим лицам, юридическим лицам и, возможно, к самим роботизированным системам (например, деактивация или уничтожение)².

Осложняющими факторами в этом контексте являются возможность самообучения программ ИИ (которое может и должно быть ограничено), а также скорость, качественные и количественные показатели развития ИИ.

В случае трансграничного характера преступлений такого рода может оказаться неэффективной и существующая система международного сотрудничества по вопросам выдачи и оказания правовой помощи по соответствующим уголовным делам, в частности, ввиду необходимости соблюдения принципа двойной наказуемости (*double criminality*), сбора, хранения, передачи и использования электронных доказательств, с учетом возможной некооперабельности компаний-производителей в предоставлении необходимых сведений в рамках сотрудничества с правоохранительными органами (что выявилось, например, в процессе сотрудничества с Интернет-провайдерами). Возникает и ряд вопросов, связанных с обеспечением защиты персональных данных и коммерческой тайны.

Анализ опыта ряда государств-участников СЕ в этой сфере показал отсутствие комплексного правового регулирования, что соответствующие юридические нормы либо полностью отсутствуют (в большинстве случаев) либо регулируют лишь отдельные вопросы (например, сертификацию или лицензирование использования «беспилотных автомобилей»)³.

Следует отметить, что перенасыщенность тематической сессии ЕКПП выступлениями экспертов фактически не позволила участникам провести «плотное» обсуждение выявленных проблем, что во многом свело ее к «введению в тему».

В результате ЕКПП принято решение продолжить работу на данном направлении и создать экспертную рабочую группу из 15 членов, которая должна выработать своего рода «дорожную карту» по решению выявленных проблем и определить роль Комитета в этом процессе.

Указанная группа, в которую вошел и российский представитель, 27 марта 2019 г. провела свое первое заседание, на котором был подготовлен вопросник, который позволит собрать для последующего анализа информацию об опыте, имеющемся в данной сфере в государствах-членах Совета Европы, а также государствах-наблюдателях, включая Канаду, США и Японию.

Говоря о проблемах, связанных с применением «беспилотных автомобилей» (в т. ч. о возможности злонамеренного вмешательства в управление такими автомобилями),

¹ Об общих правовых проблемах, связанных с ИИ, см.: Морхат П. М. Искусственный интеллект: правовой взгляд: научная монография / РОО «Институт государственно-конфессиональных отношений и права». М.: Буки Веди, 2017. 257 с.

² См., например: Кибальник А. Г. Как уголовное право будет реагировать на появление искусственного интеллекта? // Уголовное право: стратегия развития в XXI веке: материалы XVI Международной научно-практической конференции. Москва: РГ-Пресс, 2019. С. 59-63.

³ Подробнее см. документ Совета Европы CDPC(2018)22, Strasbourg, 28 Nov. 2018.

следует отметить существование и появление в ближайшем будущем научных и технологических разработок (в частности, в области робототехники и биологии, в т. ч. в генной инженерии¹), которые при попадании в руки преступников (включая террористов) могут причинить гораздо более серьезный ущерб людям и обществу. Примером, являются уже имеющиеся образцы дронов, осуществляющих целенаправленный поиск (на основе технологий распознавания лица) и убийство отдельных людей.

В связи с этим, по нашему мнению, необходимо поставить вопрос об организации на постоянной основе на национальном и международном уровнях (желательно в рамках ООН) работы по криминологическому прогнозированию возможного использования достижений науки и техники в преступных целях. С тем чтобы иметь возможность заранее принимать необходимые превентивные меры, включая законодательные, в т. ч. связанные с криминализацией (по возможности, упреждающей) соответствующих общественно-опасных деяний.

В России такая работа могла бы осуществляться в рамках специального совета по данной проблематике или национального совета по уголовной политике и предупреждению преступности, который целесообразно создать при Президенте Российской Федерации² или при Правительстве Российской Федерации с учетом Федерального закона от 23.06.2016 № 182-ФЗ «Об основах системы профилактики правонарушений в Российской Федерации»³.

Список литературы

1. Баранчикова М. В. Проблемы квалификации дорожно-транспортных преступлений, совершённых с участием беспилотных транспортных средств // Уголовное право: стратегия развития в XXI веке: материалы XVI Международной научно-практической конференции. Москва: РГ-Пресс, 2019. С. 8-12.
2. Кибальник А.Г. Как уголовное право будет реагировать на появление искусственного интеллекта? // Уголовное право: стратегия развития в XXI веке: материалы XVI Международной научно-практической конференции. Москва: РГ-Пресс, 2019. С. 59-63.
3. Коробеев А. И., Чучаев А. И. Вред, причиненный роботомобилем: уголовно-правовые проблемы // Уголовное право: стратегия развития в XXI веке: материалы XVI Международной научно-практической конференции. Москва: РГ-Пресс, 2019. С. 63-70.
4. Морхат П. М. Искусственный интеллект: правовой взгляд: научная монография / РОО «Институт государственно-конфессиональных отношений и права». М.: Буки Веди, 2017. – 257 с.

¹ Тищенко Е. В., Фролова Е. Ю. Риски криминального использования биотехнологий // Будущее российского права: концепты и социальные практики. V Московский юридический форум. XIV. Международная научно-практическая конференция (Кутафинские чтения): материалы конференции: в 4 ч. Часть 3. Москва: РГ-Пресс, 2018. С. 244-248.

² Например, в странах Северной Европы созданы советы (комиссии) по предупреждению преступности (с включением представителей академических кругов и профильных общественных организаций). А при Президенте США действует Консультативный совет по науке и технике (the President's Council of Advisors on Science and Technology – the PCSAST), который занимается и уголовно-правовыми вопросами. В частности, в сентябре 2016 г. Совет опубликовал доклад «Судебно-медицинская экспертиза в судах по уголовным делам: обеспечение научной обоснованности сравнительных методов», в котором поставил под сомнение научную обоснованность некоторых применяемых в США методик судебно-медицинской экспертизы (см.: https://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_forensic_science_report_final.pdf).

³ Об основах системы профилактики правонарушений в Российской Федерации: Федеральный закон от 23.06.2016 № 182-ФЗ // Официальный интернет-портал правовой информации <http://www.pravo.gov.ru> [Электронный ресурс]. Режим доступа: <http://pravo.gov.ru/proxy/ips/?docbody=&nd=102402071> (дата обращения: 18.05.2019).

5. Тищенко Е. В., Фролова Е. Ю. Риски криминального использования биотехнологий // Будущее российского права: концепты и социальные практики. V Московский юридический форум. XIV. Международная научно-практическая конференция (Кутафинские чтения): материалы конференции: в 4 ч. Часть 3. Москва: РГ-Пресс, 2018. С. 244-248.

6. Штаге Д. Автоматизированное вождение и спорные ситуации // Уголовное право: стратегия развития в XXI веке: материалы XVI Международной научно-практической конференции. Москва: РГ-Пресс, 2019. С. 3-7.

Vladimir V. Zimin

Assistant of Golovinsky Interdistrict Public Prosecutor of Moscow,
Postgraduate Student, University of the Prosecutor's Office of the Russian Federation
(Russia, Moscow)
nivolkovis@gmail.com

SCIENTIFIC AND TECHNICAL ACHIEVEMENTS AND CRIMES OF THE FUTURE: ISSUES OF CRIMINOLOGICAL FORECASTING AND PRE-EMPTIVE CRIMINALIZATION

Abstract: The report stands up for criminal law needs giving hard response to crimes related to artificial intelligence (AI) and cybercrime. The imperatives of personal data protection, artificial intelligence and human rights within future context of technological convergence require new methods of tracking information. Even now it's already widely used by drones and by automatic control of vehicles conducting. It is proposed to create on a permanent basis under the auspices of the UN Institute, capable of keeping not only the possible utilization of the most recent scientific and technical developments for anti-crime, but also the possible prevention of criminality on the basis of forecasting events.

Keywords: UN, AI, drones, robots, Budapest convention, double criminality, road map, electronic proofs, autonomous vehicles.

Коваленко Ксения Евгеньевна

Кандидат юридических наук,
доцент кафедры трудового, экологического права и гражданского процесса
Алтайский государственный университет
(г. Барнаул)
Kovalenko1288@mail.ru

Коваленко Наталья Евгеньевна

Студент Юридического института
Алтайский государственный университет
(г. Барнаул)
kovalenkorub5@gmail.com

Кузьмина Анна Сергеевна

Кандидат психологических наук, старший преподаватель кафедры клинической
психологии
Алтайский государственный университет
(г. Барнаул)
annakuz87@yandex.ru

**ВВЕДЕНИЕ В ПРОГРАММУ ПОДГОТОВКИ ВОДИТЕЛЕЙ ЭЛЕКТРОННЫХ
СИСТЕМ ОБУЧЕНИЯ***

Аннотация: проблема нарушения правил дорожного движения в наше время становится одной из важнейших в обеспечение безопасности граждан. Способность к овладению навыкам безопасного вождения лишь частично ограничивается психологией водителей и может быть частично компенсировано интенсивными занятиями по приобретению водительского опыта. Экстремальный характер деятельности водителей подчеркивается широко обсуждаемыми вопросами личностного фактора в обеспечении безопасности дорожного движения. Задача и вызов состоит в том, чтобы, используя лучшие практики, приобрести водительскую практику в относительно безопасных условиях.

Ключевые слова: безопасность, правила дорожного движения, искусственный интеллект, электронная система, контраварийное вождение.

Формирование безопасной модели поведения особенно нужно на начальной стадии процесса, чтобы изменить отношение к безопасности у критического большинства населения. При этом основной акцент должен быть сделан на личной заинтересованности водителей в решении проблемы безопасности дорожного движения, на необходимости разумного, ответственного и дисциплинированного поведения на дорогах, внимания участников дорожного движения друг к другу, показа позитивных фактов культуры и мастерства вождения.

Несмотря на снижение различных показателей аварийности дорожного движения в России в целом, и Алтайском крае в частности, показатели смертности за 11 месяцев 2018 года в дорожно-транспортных происшествиях в Алтайском крае составляет 257 человек, что только на 15% ниже в сравнении с 12 месяцами 2017 года¹. Большинство происшествий на дороге связано с человеческим фактором, среди которых можно назвать психологические и

* Исследование выполнено при поддержке гранта Президента Российской Федерации для государственной поддержки молодых российских ученых МК-5088.2018.6.

¹ Евтюков С. А., Васильев Я. В. Реконструкция и экспертиза ДТП в примерах. СПб.: Петрополис, 2018. 180 с.

психофизиологические показатели человека, такие как уровень внимания, психоэмоциональное состояние, произвольная регуляция поведения, личностные показатели. Человеческий фактор в осмыслении вопросов высоко рискованного вождения осмысливается в транспортной психологии. Делаются попытки раскрытия и описания роли человеческого фактора в осуществлении высоко рискованного вождения (О.В. Ариничева, Е.М. Каймакова), внедряются методы инструментальной оценки квалификации водителей (Б.Д. Ефремов, Ю.В. Оверин), в рамках профилактики ДТП разрабатываются педагогические основы подготовки водителей автотранспортных средств (С.А. Евтюков, Ю.И. Лобанова). Ю.В. Денисова, Ю.Ю. Голубихина, Н.А. Гончарова исследуют личностные возможности и способности водителей адекватно реагировать в экстремальных дорожных ситуациях (на уровне показателей подвижности и силы нервной системы, перцептивных особенностей)¹.

С увеличением количества водителей, растет и вероятность дорожно-транспортных происшествий. Тем не менее, говорить, что основной проблемой возникновения аварийности – это увеличение количества водителей нельзя. Естественно, что с увеличением одного элемента, увеличивается другой. Нас будет интересовать одна из первопричин аварийности, которая появляется у водителей-новичков.

26 декабря 2013 г. был принят приказ Министерства образования и науки РФ от N 1408 «Об утверждении примерных программ профессионального обучения водителей транспортных средств соответствующих категорий и подкатегорий»², который определил перечень учебных предметов базового и специального циклов с указанием времени, отводимого на освоение учебных предметов, включая время, отводимое на теоретические и практические занятия для водителей транспортных средств 26 категории и подкатегорий. Теперь, чтобы продолжить образовательную деятельность, автошкола должна пройти проверку сотрудниками ГИБДД и получить от них соответствующее разрешение. Без данного разрешения школа оказывается нелегальной, и выпускники таких учебных заведений не смогут сдать экзамен в ГИБДД и получить водительское удостоверение³. Кроме того, изменилась и процедура получения водительских прав.

По мнению, сотрудников Госавтоинспекции и Министерства науки и высшего образования РФ, данная реформа поможет повысить качество образования в автошколах и сократить количество ДТП среди молодых водителей⁴. Однако на сегодняшний день следствием таких реформ стало пока лишь банкротство некоторых автошкол и значительное повышение стоимости обучения, но не повышение правовой культуры водителей транспортных средств⁵.

Причиной повышенной аварийности является недостаточная подготовка водителей в автошколах. В современных программах подготовки водителей содержатся следующие модули:

- базовый,

¹ См.: Борисова С. Е. Влияние психологических установок водителей на безопасность дорожного движения // Психология и права. 2011. № 4. С. 3-12; Горбачев М. С. Экстремальное вождение: Гоночные секреты. М.: Престиж книга, 2006. 304 с.; Дятлов М. Н. Электронные системы обучения водителя транспортного средства // Молодой ученый. 2013. № 3. С. 52-56; Евтюков С. А., Васильев Я. В. Реконструкция и экспертиза ДТП в примерах. СПб.: Петрополис, 2018. 180 с.; Ермолаев В. В., Макушина О. П., Четверикова А. И. Социально-психологические детерминанты проявления агрессии водителями пассажирского транспорта на российских дорогах // Социальная психология и общество. 2013. № 2. С.108-118; Ефремов Б. Д., Оверин Ю. В. Метод инструментальной оценки квалификации водителей // Техничко-технологические проблемы сервиса. 2012. Вып. 3. Т. 2. С. 51-55; Каминский А. Мастер вождения автомобиля. М., 2013. 240 с.

² Об утверждении примерных программ профессионального обучения водителей транспортных средств соответствующих категорий и подкатегорий: приказ Министерства образования и науки РФ от 26 декабря 2013 г. N 1408 // Российская газета. 2014. N 172/1.

³ Майоров В. И. Государственно-правовое обеспечение безопасности дорожного движения в РФ: теоретико-прикладные проблемы: монография. М.: Юрлитинформ, 2018. 208 с.

⁴ Эрганова Н. Е. Методика профессионального обучения: учеб. пособие. М.: Изд-во «Академия», 2017. 160 с.

⁵ Лобанова Ю. И. Стиль вождения: определяющие факторы, характеристики, направления оптимизации // Российский гуманитарный журнал. 2015. Т. 4. № 1. С. 76-84.

- специализированный и
- профессиональный.

В рамках этих модулей, на наш взгляд, проходит сильно теоретизированная подготовка водителей к реальным условиям вождения. На них идет обучения законодательству, устройству автомобиля и оттачивания навыков вождения в рамках городского движения или на полигоне. В этих условиях водитель не сталкивается с редкими ситуациями, которые могут его ожидать после выпуска из автошколы. Так как во время обучения рядом с ним находится инструктор, который подсказывает, что необходимо сделать и не дает сделать раковых ошибок.

Причиной аварий в наше время является человеческий фактор. После выпуска водитель-новичок чувствует себя скованно, напряженно. Рядом нет инструктора, который мог бы помочь. В г. Барнауле эти факторы могут проявляться еще сильнее, чем в г. Белокурихе, что связано с плотным потоком машин и интенсивностью движения. Это в совокупности давит на водителя, и, следовательно, он делает в спешке ошибки, которые прямо или косвенно влияют на ДТП. Интенсивность движения опасна еще и тем, что другие водители могут производить резкие передвижения по полосам, без указания сигналов или показывая их несвоевременно.

Еще одной причиной необходимости введения электронной системы обучения котраварийного вождения является климатические условия г. Барнаула. В нашем регионе явно выражены различные сезоны года. Это также влияет на аварийность. От тех или иных погодных условий зависит стиль вождения, скорость, приемы, используемые для предотвращения.

Для обогащения практического опыта претендента на получение водительского удостоверения и уменьшения актуальности вышеперечисленных проблем, и необходимо ввести электронную систему обучения, как контраварийное (экстремальное) вождение, которое выполнялось бы на электронном тренажере. Использование современных информационных технологий должно стать неотъемлемым элементом в современной подготовки водителей¹. Электронная система обучения «контраварийное (экстремальное) вождение» позволит приблизить условия обучения к реальным, не подвергая учащегося и инструктора опасности. Кроме того, он позволит использовать индивидуальный подход к каждому из обучаемых и допуская многократное повторение отдельных операций по управлению автомобилем, добиваясь четкого их выполнения. Используя автотренажеры, можно разбить сложный процесс вождения на отдельные элементы и воспроизвести аварийные ситуации, отработка которых на автодроме и на дороге сопряжена с опасностью, а также уменьшить расходы на обучение водителя. Основная задача тренажерного этапа подготовки «контраварийное (экстремальное) вождение» — выработать у учащегося в безопасных условиях элементарные начальные зрительно-двигательные навыки управления автомобилем и восприятия среды движения. Поэтому при обучении изучаются основные, базовые навыки управления автомобилем, которые отрабатываются более подробно на следующих этапах подготовки водителей.

Электронная система обучения будет направлена на получение водителями опыта вождения в различных ситуациях, которые могут по той или иной случайности произойти с ним за рулем. На данных курсах водитель будет оттачивать свои навыки в экстремальных условиях, когда ему необходимо за короткое время принять правильное решение. Закрепить необходимо следующие ситуации:

1. Резкое прохождение препятствий. Это поможет водителю, в ситуациях, когда его подрезал другой водитель или на дорогу неожиданно выбежал пешеход и т. д. Это помогло бы избежать аварии, либо уменьшить ущерб от нее.

¹ Дятлов М. Н. Электронные системы обучения водителя транспортного средства // Молодой ученый. 2013. № 3. С. 52-56.

2. Езда на льду и скользкой дороге. Каждый год с приходом зимы на дорогах происходит множество аварий по причине заноса автомобиля при торможении, повороте, перестроении и т. д. Это связано в какой-то степени с тем, что водители попросту теряются в таких ситуациях и не знают, как действовать, либо им не хватает опыта.

3. Применение экстремального торможения на скользкой дороге.

4. Спуск с крутых склонов.

5. Прохождение водных объектов.

Это малая часть того, что можно предложить для включения в электронную систему обучения «контраварийное (экстремальное) вождение». Если данная система будет внесена в обязательную программу, то у водителя будет формироваться реакция на экстренные ситуации, будет заготовлен рефлексный план действий. При управлении транспортным средством не будет ощущаться скованность, растерянность, так как водитель уже будет знать, что ему делать.

Конечно же, это будет полезно в совокупности с соблюдением правил дорожного движения. Разработанные элементы могут применяться не только при обучении начинающих водителей, но и при тестировании для оценки водительского мастерства при непрерывной подготовке водителей автомобиля.

Список литературы

1. Борисова С. Е. Влияние психологических установок водителей на безопасность дорожного движения // Психология и права. 2011. № 4. С. 3-12.

2. Горбачев М. С. Экстремальное вождение: Гоночные секреты. М.: Престиж книга, 2006. 304 с.

3. Дятлов М. Н. Электронные системы обучения водителя транспортного средства // Молодой ученый. 2013. № 3. С. 52-56.

4. Евтюков С. А., Васильев Я. В. Реконструкция и экспертиза ДТП в примерах. СПб.: Петрополис, 2018. 180 с.

5. Ермолаев В. В., Макушина О. П., Четверикова А. И. Социально-психологические детерминанты проявления агрессии водителями пассажирского транспорта на российских дорогах // Социальная психология и общество. 2013. № 2. С. 108-118.

6. Ефремов Б. Д., Оверин Ю. В. Метод инструментальной оценки квалификации водителей // Техничко-технологические проблемы сервиса. 2012. Вып. 3. Т. 2. С. 51-55.

7. Каминский А. Мастер вождения автомобиля. М., 2013. 240 с.

8. Лобанова Ю. И. Стиль вождения: определяющие факторы, характеристики, направления оптимизации // Российский гуманитарный журнал. 2015. Т. 4. № 1. С. 76-84.

9. Майоров В. И. Государственно-правовое обеспечение безопасности дорожного движения в РФ: теоретико-прикладные проблемы: монография. М.: Юрлитинформ, 2018. 208 с.

10. Эрганова Н. Е. Методика профессионального обучения: учеб. пособие. М.: Изд-во «Академия», 2017. 160 с.

Ksenia E. Kovalenko

PhD in Law, Associate Professor of the Department of Labor, Environmental Law and Civil Procedure

Altai State University

(Russia, Barnaul)

Kovalenko1288@mail.ru

Kovalenko Natalia Evgenievna

Student of Law Institute

Altai State University
(Russia, Barnaul)
kovalenkorub5@gmail.com

Kuzmina Anna Sergeyevna
PhD in Psychology, Senior Lecturer of the Department of Clinical Psychology
Altai State University
(Russia, Barnaul)
annakuz87@yandex.ru

INTRODUCTION TO THE DRIVERS TRAINING PROGRAM ELECTRONIC SYSTEMS

Abstract: the problem of traffic violations in our time to become one of the most important in ensuring the safety of citizens. The ability to master the skills of safe driving is only partially limited by the psychology of the drivers and can be partially compensated for by intensive lessons in gaining driving experience. The extreme nature of the activities of drivers is emphasized by the widely discussed issues of the personal factor in ensuring road safety. The challenge to use the best practices to acquire driving practice in relatively safe conditions.

Keywords: safety, rules of the road, artificial intelligence, electronic system, emergency driving.

Кодан Сергей Владимирович

Доктор юридических наук, профессор, профессор кафедры теории государства и права
Уральский государственный юридический университет
(г. Екатеринбург)
svk2005@yandex.ru

ИНФОРМАЦИОННЫЙ ПОДХОД В ЮРИДИЧЕСКОМ ИСТОЧНИКОВЕДЕНИИ*

Аннотация: В статье рассматривают вопросы понимания и определения места и роли информационного подхода в юридическом источниковедении. Через призму междисциплинарного взаимодействия социально-гуманитарных наук акцентируется внимание на инструментальных характеристиках и возможностях использования информационного подхода в исследовательских практиках, связанных с использованием информационных ресурсов. Характеризуются основные понятия в контексте анализируемого методологического подхода.

Ключевые слова: информатика, информационные ресурсы, юриспруденция, юридическое источниковедение, источники познания.

Качественно новое состояние современного общества с развитием в нем информационных процессов ведет к формированию информационного общества, определяемого в науке «как цивилизация, в основе существования и развития которой лежит особая нематериальная субстанция, именуемая информацией, обладающая свойством взаимодействия как с материальным, так и духовным миром человека»¹. Изучение и использования носителей информации юридической направленности в современных условиях просто немыслимо без работы в информационном пространстве. В связи с этим необходимо обозначить ряд проблем, связанных с использованием информационного подхода в юридическом источниковедении. При этом заметим, что информационный подход в социогуманитаристике опирается на ряд положений, характеризующих его место в методологии источниковедения. Указанное требует обращения к двум категориям - методологический подход и информационный подход.

Методологический подход в целом выступает в качестве практико-ориентированной стратегии работы ученого и представляет, как отмечает Э. Г. Юдин, «принципиальную методологическую ориентацию исследования, как точку зрения, с которой рассматривается объект изучения»². В контексте указанного Н. Н. Тарасов обращает внимание на то, что «методологический подход представляет скорее не «изображение» объекта, а «изображение» научного мышления, изображающего объект» и указывает, что «методологический подход направлен не на видение объекта, как объект исследования устроен «на самом деле», а на организацию исследовательских средств, обеспечивающих требуемое видение, т.е. способ «помыслить» объект. Способ помыслить объект исследования и есть то, что в литературе, характеризуя методологический подход, называют принципиальной методологической ориентацией научного исследования, точкой зрения на объект, понятием или принципом, задающим общую стратегию

* Исследование выполнено при финансовой поддержке Российского фонда фундаментальных исследований в рамках научного проекта № 18-011-00329 «Юридическое источниковедение: теория, методология и методика изучения носителей государственно-правовой информации».

¹ Лукина Н. П. Методологический потенциал информационного подхода в современном научном познании // Гуманитарная информатика. 2011. Вып. 6. С. 8-9.

² Юдин Э. Г. Методология науки. Системность. Деятельность. М., 1997. С. 69.

исследования»¹. В указанном значении могут выступать системный, информационный, деятельностный, синергетический и др. подходы.

Методологический подход как инструмент исследования позволяет в соответствии с целями и задачами работы выбрать соответствующий им конкретный подход и, опираясь на предмет определяющей его исходной научной дисциплины, сфокусировать внимание на какой-либо стороне объекта познания. Подход в контексте междисциплинарной направленности исследования и привлечения инструментария других областей науки обеспечивает взаимодействие наук, что «является необходимой и актуальной потребностью развития самой науки, повышения качества, эффективности и результативности научных исследований» - справедливо подчеркивает Д. А. Керимов². При этом следует учитывать, что методологический подход «является сложной исследовательской моделью, претендующей на определенную целостность получаемых в результате его реализации знаний»³. В итоге, по мнению Г. П. Щедровицкого, появляется «новое изображение объекта», которое характеризуется тем, что «оно собрало и объединило в себе все то объективное содержание, которое было зафиксировано в уже имевшихся ранее знаниях», «его структура была введена как «основание» и «источник» всех проявлений объекта, обнаруживаемых в прямом познавательном оперировании с этим объектом» и «на основе особого познавательного оперирования с самим этим изображением и выраженным в нем предметом знания выводились и обосновывались новые сложные знания об объекте»⁴.

Методологический подход на уровне взаимодействия различных наук позволяет обеспечить выход за пределы традиционного рассмотрения государственно-правовых явлений и институтов преимущественно в рамках юридической догматики и дополнить, расширить представления о них на основе привлечения знаний из других наук. При этом важно учитывать замечание известного российского юриста-методолога В. М. Сырых – «Правоведам приходится заимствовать методы научного познания, разрабатываемые математикой, статистикой, социологией и другими науками. Понятно, что все заимствованные методы научного познания оказывают позитивное влияние в той мере, в какой правоведам удастся их конкретизировать к специфике познания правовых явлений и их закономерностей и наоборот»⁵.

Информационный подход в научном познании является специальным методологическим средством и выступает как «общая ориентация ученого на анализ именно информационного «среза» действительности» – подчеркивает Э. П. Семенюк. Он также отмечает, что при его использовании в исследовательских практиках «задачей исследования в конечном счете является раскрытие специфически неповторимой информационной роли каждого конкретного феномена во всем его богатстве свойств и отношений»⁶. Указанный поход в стратегии исследования, как отмечает американский психолог Джером Брунер, означает «некоторый способ приобретения, сохранения и использования информации, служащей достижению определенных целей в том смысле, что он должен привести к определенным результатам»⁷. Указанное нацеливает исследователя в методологическом плане на достаточно широкий спектр содержательных характеристик указанного подхода, которые опираются на его семантическое ядро (слово «информационный»), которое дает название подходу и служит ориентиром для выбора его

¹ Тарасов Н. Н. Методологические проблемы юридической науки. Екатеринбург, 2001. С. 233-234.

² Керимов Д. А. Проблемы общей теории государства и права. М., 2007. С. 12.

³ Тарасов Н. Н. Указ соч. С. 239.

⁴ Щедровицкий Г. П. Избранные труды. М., 1995. С. 653-657.

⁵ Сырых В. М. История и методология юридической науки. М., 2012. С. 45.

⁶ Семенюк Э.П. Информационный подход к познанию действительности. Киев, 1988. С. 8.

⁷ Брунер Дж. Психология познания. За пределами непосредственной информации. Пер. с англ. М., 2008. С. 136.

как методологического инструмента. Поэтому должны быть учтены ряд понятий и научных взаимодействий, непосредственно связанных с данным подходом.

Понятие информации находится в непосредственной связи с информационным подходом. С конца 1940-х гг. «информация» рассматривается как самостоятельная научная категория (К. Шеннон, Н. Винер и др.) и в настоящее время активно исследуется в различных научных дисциплинах¹. Понятие информации является одним из фундаментальных понятий науки и не имеет однозначного определения. В рамках данной статьи используем понятие информации семантической направленности, которое определяет В. Г. Афанасьев – по его мнению информация «представляет собой знания, сообщения, сведения о социальной форме движения материи и обо всех её других формах в той мере, в какой они используются обществом, человеком, вовлечены в орбиту общественной жизни»². Составной частью информации является *социальная информация*, которая «используется для обозначения совокупности человеческих знаний, представлений, сообщений о социальных процессах, которые выступают в сигнальной форме, форме сообщений, и активно используются людьми в своей жизнедеятельности»³.

Информатика в контексте информационного подхода в качестве науки связана с его технической реализацией при помощи аппаратных средств – компьютера, программного обеспечения и различного оборудования, обеспечивающего получение, хранение и передачу информации. В данном плане интерес представляют и постоянно возрастающие возможности расширяющегося набора инструментов, необходимых для получения и обработки информации, полученной из различного рода источников. На стыке ряда естественных и социально-гуманитарных наук возникла и активно развивается в качестве нового междисциплинарного научного направления *социальная информатика*, ориентированная на изучение видов и форм проявления информации в обществе, информационные процессы, технологии, системы и коммуникации, которые имеют значимость для жизнедеятельности человека и общества⁴.

Информационный обмен, находясь в пространстве исследования информационного подхода, ориентирует исследователя на передачу информации. При этом необходимо выделить две проекции информационного обмена. Информационный обмен осуществляется *по горизонтали* – в режиме настоящего времени и имеет непосредственный характер и характеризуется синхронным движением информации, обеспечивающей прямую и обратную связь между субъектами коммуникации и *по вертикали* – в режиме ретроспективного, опосредованного через носители получения информации, когда движение информации имеет диахронный характер и характеризуется передачей информации от поколения к поколению, обеспечивая преемственность социального опыта, знаний и традиций в истории развития общества. Особое значение имеет информационный обмен в области науки – *научно-информационная деятельность*, под которой понимается «организационно оформленная разновидность научного труда который выполняется в целях повышения эффективности собственно исследований и разработок и заключается в сборе, аналитико-синтетической переработке, хранении и поиске закреплённой в документах научной информации, а также в представлении этой научной информации ученым-исследователям в соответствующее время и в удобной для них форме»⁵. Особенно значимым для развития информационного обмена в сфере научных исследований стало появление глобальных сетей передачи информации и

¹ См.: Соколов А.В. Информационное общество в виртуальной и социальной реальности. СПб., 2011.

² Афанасьев В. Г. Социальная информация. М., 1994. С. 13.

³ Журавлев Г. Т., Шабельская А. В. Общее понятие социальной информации // В мире научных открытий. 2010. № 4-16 (10). С. 61-62. Режим доступа: <http://naukarus.com/obschee-ponyatie-sotsialnoy-informatsii> (дата обращения 10.05.2019).

⁴ См.: Урсул А. Д. Информатизация общества. Введение в социальную информатику. М., 1990.

⁵ Михайлов В. И., Черный А. И., Гиляревский Р. С. Научные коммуникации и информатика. М., 1976. С. 240-241.

информационных баз данных, которые обеспечили широчайшие возможности доступа к информации социально-гуманитарного характера, включая и многочисленные источники, прямо или косвенно связанные с юридической сферой жизнедеятельности общества. При этом ранее территориально локализованные места хранения носителей информации на уровне отдельных архивов и библиотек, отдаленных друг от друга территориально, получили возможность предоставить свои ресурсы первоначально на уровне каталогов, а с оцифровкой материалов и в виде электронных документов широкому кругу пользователей. В цифровую эпоху, как отмечает канадский философ и филолог Герберт Маклюэн, «технология фрагментированных процессов внезапно слилась воедино с человеческим диалогом и потребностью во всепоглощающем внимании к человеческому единству. Люди вдруг превратились в кочевых собирателей знания, кочевых, как никогда раньше, информированных, как никогда раньше, свободных от фрагментарного специализма, как никогда раньше, - и вместе с тем, как никогда раньше, вовлеченных в тотальный социальный процесс»¹.

Информационный подход в юридическом источниковедении основывается на методологии изучения носителей социальной информации, формирование которой было связано с теоретическими наработками в сфере исторического источниковедения ученых-историков советского и постсоветского периодов развития отечественной исторической науки. С середины 1970-х гг. усилиями историков Л. Н. Пушкарева² и, особенно, И. Д. Ковальченко³ информационный подход в изучении исторических источников выделился в самостоятельное направление в источниковедении и перешел в плоскость методологии истории исторического познания. Развитие информационного подхода получило развитие в работах О. М. Медушевской в рамках созданной ею когнитивно-информационной теории источниковедения⁴.

В основе информационного подхода И. Д. Ковальченко находится тезис – «В самом широком плане под информацией понимают всю совокупность сведений, которые содержатся в исторических источниках, или, говоря иначе, информация – результат отражения современниками исторической действительности». Он, акцентируя внимание на информационных механизмах появления носителей исторической информации, показывает объектно-субъектную, целевую и хронологическую составляющую в образовании носителей информации - «Возникновение большинства исторических источников представляет собой информационный процесс, в котором фигурируют объект - отражаемая реальность, субъект - творец источника и информация – результат отражения объекта субъектом. Этот процесс, как и всякий информационный, всегда имеет прагматический аспект, т.е. творец источника всегда преследует определенную цель, выявляя сведения об объективной действительности. Эти сведения требуются для решения тех или иных общественных или личных задач. То, что потом стало исторической информацией, зафиксированной в исторических источниках, первоначально являлось информацией, необходимой для удовлетворения практических нужд. Это в одинаковой мере относится и к законодательству, и к правовым актам, фиксировавшим и регулировавшим те или иные отношения, и к личной переписке, и к мемуарам, которые преследовали цель самовыражения, самосознания и самоутверждения личности»⁵. На основе указанного подхода в научный оборот и образовательный процесс было введено понятие – «Исторические источники - это всё, отражающее развитие человеческого общества и являющееся основой для его научного познания, т.е. всё, созданное в процессе

¹ Маклюэн Г. М. Понимание Медиа. Внешние расширения человека. Пер. с англ. М., 2003. С. 412.

² См.: Пушкарев Л. Н. Классификации русских письменных источников по отечественной истории. М., 1975.

³ Ковальченко И. Д. Исторический источник в свете учения об информации (к постановке проблемы) // История СССР. 1982. № 3. С. 129-148.

⁴ Медушевская О. М. Теория и методология когнитивной истории. М., 2008.

⁵ Ковальченко И. Д. Методы исторического исследования. Изд. 2-е. М., 2003. С. 127-128.

человеческой деятельности и несущее информацию о многообразных сторонах общественной жизни»¹.

Информационный подход в современном источниковедении базируется на научном синтезе теории информации и когнитивных наук (изучающих человеческое мышление и исходит из того, что существует информационная сфера жизнедеятельности общества в которой собственно и создаются продукты человеческой деятельности как материально-вещественные внешние формы выражения мышления и которые выступают как источники познания социальной действительности. О. М. Медушевская, обращая внимание на информационную функцию источника, рассматривает его в качестве своеобразного «информационного посредника» – «Связь между человеком и социумом через созданный одним и прочитанный «другими» интеллектуальный продукт предстает как эволюционно и глобально значимая: каждый созданный интеллектуальный продукт уже в момент своего создания пополняет совокупный ресурс человечества и может быть актуализирован теперь и всегда». В этом плане источниковедение рассматривается как «эмпирическая гуманитарная наука, объектом которой являются интеллектуальные продукты, созданные в ходе целенаправленной человеческой деятельности, а предметом – конкретная содержательная значимость их информационного ресурса как источников для изучения человека, общества и мира в целом»². Именно в данном плане – как интеллектуальные продукты - и используются в юридическом исследовании носители государственно-правовой информации.

Информационный подход в юридическом источниковедении исследования реализуется через знание его возможностей и подбор необходимых средств и инструментов для поиска и проведения исследования носителей информации. Он предполагает использование возможностей информационных средств работы с источниками, различных электронных баз данных и, особенно, информационных порталов «Гарант», «Консультант Плюс», «Кодекс» и др.

Итак, обозначенные характеристики и возможности информационного подхода в юридическом источниковедении показывают его значение в изучении носителей государственно-правовой информации. Данный подход ориентирует исследователя в информационном пространстве на уровне знаний и навыков для их использования в научной работе.

Список литературы

1. Афанасьев В. Г. Социальная информация. М., 1994.
2. Брунер Дж. Психология познания. За пределами непосредственной информации. Пер. с англ. М., 2008.
3. Журавлев Г. Т., Шабельская А. В. Общее понятие социальной информации // В мире научных открытий. 2010. № 4-16 (10). С. 61-62. Режим доступа: <http://naukarus.com/obschee-ponyatie-sotsialnoy-informatsii>
4. Источниковедение истории СССР. Учебник / под ред. И.Д. Ковальченко. 2-е изд. М., 1981.
5. Керимов Д. А. Проблемы общей теории государства и права. М., 2007.
6. Ковальченко И. Д. Исторический источник в свете учения об информации (к постановке проблемы) // История СССР. 1982. № 3. С. 129-148.
7. Ковальченко И. Д. Методы исторического исследования. Изд. 2-е. М., 2003.
8. Лукина Н. П. Методологический потенциал информационного подхода в современном научном познании // Гуманитарная информатика. 2011. Вып. 6. С. 6-22.

¹ Источниковедение истории СССР. Учебник / под ред. И.Д. Ковальченко. 2-е изд. М., 1981. С. 8.

² Медушевская О. М. Указ соч. С. 41, 352. См. также: Медушевский А. Н. Когнитивно-информационная теория как новая философская парадигма гуманитарного познания // Вопросы философии. 2009. № 10. С. 70-92.

9. Маклюэн Г. М. Понимание Медиа. Внешние расширения человека. Пер. с англ. М., 2003.
10. Медушевская О. М. Теория и методология когнитивной истории. М., 2008.
11. Медушевский А. Н. Когнитивно-информационная теория как новая философская парадигма гуманитарного познания // Вопросы философии. 2009. № 10. С. 70-92.
12. Михайлов В. И., Черный А. И., Гиляревский Р. С. Научные коммуникации и информатика. М., 1976.
13. Пушкарев Л. Н. Классификации русских письменных источников по отечественной истории. М., 1975.
14. Семенюк Э. П. Информационный подход к познанию действительности. Киев, 1988.
15. Соколов А. В. Информационное общество в виртуальной и социальной реальности. СПб., 2011.
16. Сырых В. М. История и методология юридической науки. М., 2012.
17. Тарасов Н. Н. Методологические проблемы юридической науки. Екатеринбург, 2001.
18. Урсул А. Д. Информатизация общества. Введение в социальную информатику. М., 1990.
19. Щедровицкий Г. П. Избранные труды. М., 1995.
20. Юдин Э. Г. Методология науки. Системность. Деятельность. М., 1997.

Sergey V. Kodan

Doctor of Juridical Science, Professor,
Professor of the Department of theory of state and law
Ural State Law University
(Russia, Yekaterinburg)
svk2005@yandex.ru

INFORMATION APPROACH IN A LEGAL SOURCE

Abstract: The article deals with the issues of understanding and determining the place and role of the information approach in legal source studies. Through the prism of interdisciplinary interaction focuses on the instrumental characteristics and possibilities of using the information approach in research practices related to the use of information resources. The basic concepts in the context of the analyzed methodological approach are characterized.

Keywords: Informatics, information resources, jurisprudence, legal source studies, sources of knowledge.

Колмыков Владимир Сергеевич
Студент Института экономики и права
Академия труда и социальных отношений
(г. Севастополь)
vovchik.zenit@mail.ru

ПРОБЛЕМЫ РЕАЛИЗАЦИИ ПРИНЦИПА ДОСТУПНОСТИ ЭЛЕКТРОННОГО ПРАВОСУДИЯ В ГРАЖДАНСКОМ ПРОЦЕССЕ

Аннотация: Определение круга проблем, являющихся препятствием для реализации принципа доступности электронного правосудия в гражданском процессе, и разработка путей их разрешения.

Ключевые слова: принципы, права, доступность, правосудия, судебная, защита.

Актуальность рассматриваемой проблемы, по словам автора, определяется тем, что, принципы права представляют собой «руководящие идеи, характеризующие содержание права, его сущность и назначение в обществе. Эти нормы либо прямо сформулированы в законе, либо выводятся из общего смысла законов»¹. Так как общественные отношения в силу своей природы непрерывно развиваются, правовая система должна быть адаптирована к потребностям человека и общества. Для того чтобы эти изменения были совместимы с существующей правовой системой, необходимы принципы права. Другая важная функция – это восполнение пробелов в законодательстве без принятия нормативных правовых актов. Такая ситуация возможна при аналогии права, т.е. при применении к не урегулированному в конкретной норме спорному отношению при отсутствии нормы, регулирующей сходные отношения, общих начал и смысла законодательства. Общие начала – это не что иное, как принципы права. Данное положение предусмотрено, в том числе в ч.4 ст.1 Гражданского процессуального кодекса Российской Федерации².

Автор отмечает, что в гражданском процессуальном праве особое место занимает принцип доступности правосудия. Содержащийся указание в диспозиции ч.1 ст. 4 ГПК РФ суд возбуждает гражданское дело по заявлению лица, обратившегося за защитой своих прав, свобод и законных интересов, и лишь в случаях, прямо предусмотренных законом, такое право предоставляется специально уполномоченным субъектам – прокурору, государственным органам, органам местного самоуправления и пр.

По мнению автора настоящей работы, если представить ситуацию, когда у гражданина отсутствует доступ к правосудию и подача заявления о защите нарушенного или оспариваемого права другими лицами законодательно не предусмотрена, то рассмотрение гражданского дела становится невозможным в силу отсутствия заявления, следовательно, и защита нарушенного или оспариваемого права не осуществляется. Поскольку право на доступ к правосудию является составной частью права на судебную защиту, соответственно нарушаются нормы ст.46 Конституции Российской Федерации Конституция Российской Федерации от 12.12. 1993 г.³.

Следует отметить, что по данному вопросу предпосылкой права на судебную защиту является доступность правосудия. Она следует из природы суда как власти, которой состоит в своевременном и компетентном разрешении всех правовых и социальных конфликтов, подведомственных суду. Основополагающим международным

¹ Теория государства и права / под ред. С.С. Алексеева. Москва: Норма, 2018. С. 194.

² Гражданский процессуальный кодекс Российской Федерации от 14.11.2002 г. № 138 ФЗ // СЗ РФ. 2002. № 46. Ст. 4532.

³ Конституция Российской Федерации от 12.12.1993 г. //СЗ РФ. 2014. № 31. Ст. 4398.

актом, гарантирующим доступ к правосудию, является Конвенция о защите прав человека и основных свобод, п. 1 ст. 6 которой утверждает, что каждый «в случае спора о гражданских правах и обязанностях или при предъявлении ему любого уголовного обвинения имеет право на справедливое и публичное разбирательство дела в разумный срок независимым и беспристрастным судом, созданным на основании закона»¹ [1].

Как справедливо отмечает И. А. Приходько: «проблема обеспечения доступности правосудия является многоаспектной, она имеет судеустройственную, финансовую, организационную и процессуальную стороны»². Обеспечение открытости и доступности правосудия названо в числе основных задач федеральной целевой программы «Развитие судебной системы России на 2013-2020»³. Таким образом, проблема реализации принципа доступности правосудия существует на современном этапе развития судебной системы, и государственная власть принимает попытки ее решения.

Здесь следует отметить, что доступность, прежде всего, предполагает открытость – информационную осведомленность населения о деятельности как судебной системы в целом, так и конкретного судебного учреждения. При подаче заявления перед истцом (заявителем) в первую очередь возникает вопрос о содержании заявления. Для его правильного оформления, безусловно, необходимы хотя бы минимальные знания норм ГПК РФ, поскольку нарушение требований, предъявляемых к содержанию, может обосновать оставление заявления без движения, отказ в принятии либо возвращение заявления. Таким образом, при подаче заявления в суд необходимы специальные юридические познания, которые восполняются в форме обращения за квалифицированной юридической помощью, либо достигаются самостоятельно. В гражданском процессе допускается процессуальное представительство, что также является гарантией доступного правосудия, поскольку немногие граждане в силах самостоятельно защитить свои права и законные интересы. Участие в судебном разбирательстве через представителя предполагает более эффективную правовую защиту. Однако судебное разбирательство всегда влечет за собой определенные финансовые затраты: на уплату госпошлины, оплату услуг представителя, восстановление документов и пр. Учитывая, что в России 19, 3 млн. человек согласно официальным данным имеют доход ниже прожиточного минимума⁴, для некоторых категорий граждан судебная защита своих прав ставится в зависимость от собственных материальных возможностей. Наличие институтов бесплатной юридической помощи, отсрочки и рассрочки уплаты госпошлины, освобождения от уплаты госпошлины для отдельных субъектов смягчают, в том числе и имущественное неравенство в обществе. Согласно статье 124 Конституции РФ финансирование судов производится исключительно за счет федерального бюджета.

По мнению автора, здесь следует обратить внимание на такой важный момент, что для обеспечения полного и независимого правосудия необходима хорошая материально-техническая база, которая в том числе формируется за счет уплаты заявителями госпошлины. Поэтому решение проблемы финансовой доступности правосудия видится сколько не в уменьшении размера госпошлины, а в эффективной социально-экономической политике государства по снижению уровня бедности и создание условий, обеспечивающих достойную жизнь и свободное развитие человека. В рамках упомянутой

¹ Конвенция о защите прав человека и основных свобод ETS № 005 Рим от 04.11.1950 г. (действие для РФ 05.05.1998 г.) // СЗ РФ. 2001. № 2. Ст.163.

² Приходько И. А. Доступность правосудия в арбитражном и гражданском процессе: основные проблемы. СПб: СПбГУ, 2015. С. 43.

³ О федеральной целевой программе «Развитие судебной системы России на 2013-2020 годы»: постановление Правительства Российской Федерации от 27.12.2012 г. № 1406 // СЗ РФ. 2013. № 1. Ст.13.

⁴ Численность населения с денежными доходами ниже величины прожиточного минимума // Официальный сайт Федеральной службы государственной статистики [Электронный ресурс]. Режим доступа: http://www.gks.ru/free_doc/new_site/population/urov/urov_51kv.htm. (дата обращения: 04.03.2019).

выше федеральной целевой программы 35,5% опрошенных считают информацию о деятельности судов недостаточной.

Автор считает, что пути разрешения данной проблемы видятся в создании условий для электронного судопроизводства, предусматривающего подачу в суд исковых заявлений, жалоб в электронном виде, получения копий документов и ознакомления с материалами дела, создание комплекса хранения электронных образцов судебных документов. Эффективность электронного правосудия уже доказана на практике внедрения электронной подачи документов в арбитражных судах. Наличие персональных сайтов судов также является шагом на пути формирования доступного правосудия, поскольку любой пользователь информационно-коммуникационной сети «Интернет» может отследить ход движения дела, в открытом доступе ознакомиться с судебными актами, узнать информацию об адресах и телефонах судейского аппарата.

Можно отметить, что доступ к правосудию предполагает в то же время и доступ к качественному правосудию. Тут же возникает вопрос о кадровом обеспечении судейского корпуса. Качественная сторона формирования аппарата суда обусловлена требованиями, предъявляемыми к возрасту, образованию, стажу работы, а также результатами сдачи квалификационного экзамена на должность судьи. Количественная же сторона зависит от общего количества заявлений и жалоб, поступающих в тот или иной суд. Например, в городе Севастополе за 2017 год в районные суды поступило 12 940 гражданских дел, из них 10 421 окончено; фактическое количество судей составляет 43 человека¹. Можно сделать вывод, что количество судей в Севастополе недостаточно, поскольку 81% дел завершены вынесением судебного акта, а на одного судью в течение года приходится 300 дел. Учитывая большой объем судопроизводства необходимо увеличивать штат судейского корпуса в целях качественного и быстрого правосудия. Предполагается, что гражданин, обращаясь в суд за защитой своих прав, использовал все возможные средства внесудебной защиты, поэтому вопрос о качестве правосудия – рассмотрении дела по существу в разумный срок компетентным специалистом – является основным критерием его доступности.

Следует отметить, что, по мнению автора максимальному приближению суда к населению для облегчения доступа граждан к правосудию придавалось принципиальное значение при реформировании судебной системы. Впервые Концепцией судебной реформы в Российской Федерации 1991 г. была озвучена идея образования окружных судов. Предусматривалось создание двух судебных систем: федеральной и республиканской. Федеральные окружные суды должны были служить связующим звеном республиканской судебной системы с Верховным Судом РСФСР, их юрисдикция должна была распространяться на территорию соответствующей республики. Предполагалось, что федеральные окружные суды одновременно будут судами нескольких инстанций: первой инстанции - по делам, отнесенным к их компетенции; апелляционной инстанции - для пересмотра решений районных судов, им должно принадлежать право кассационного разбирательства приговоров и решений судов республик в составе РСФСР. Иными словами, в пределах одной республики (что соответствует ныне субъекту РФ) должны были рассматриваться все жалобы, приносимые на судебные решения. Очень важно, что принцип организации окружных судов гарантировал более объективное рассмотрение, поскольку округа не должны были совпадать с административно-территориальным делением. Тем самым они выводились из-под влияния местной исполнительной власти². Данная система окружных судов будет воспринята в российскую правовую систему осенью 2019 года. После судебной реформы апелляционная и кассационная инстанции

¹ Статистический отчет за 2017 год // Официальный сайт Управления судебного Департамента г. Севастополя [Электронный ресурс]. Режим доступа: <http://usd.sev.sudrf.ru/modules.php?name=stat&id=16>. (дата обращения: 04.03.2019).

² Анишина В. И. Правосудие в современном мире: монография / под ред. В. М. Лебедева, Т. Я. Хабриевой. Москва: Норма, 2012.

будут выведены в отдельные подразделения, а дела будут рассматриваться независимо друг от друга. Для этого к 1 октября 2019 года будут созданы 5 апелляционных судов и 9 кассационных судов общей юрисдикции. Такая система разделения инстанций уже была проведена в 2003-2006 годах, когда после принятия Федерального конституционного закона «О внесении изменений и дополнений в Федеральный конституционный закон «Об арбитражных судах в Российской Федерации», был создан 21 новый арбитражный апелляционный суд¹.

Автор считает, такое совершенствование судебной системы позволит, во-первых, обеспечить идентичность с системой арбитражных судов (которая на сегодняшний день более развита по сравнению с общей юрисдикцией); во-вторых, более соответствует принципу разделения властей и принципу независимости судебного разбирательства.

Надо подчеркнуть, что, доступность суда можно рассматривать как совокупность условий, создающих возможность для беспрепятственного обращения всякого заинтересованного лица в суд за защитой своих нарушенных или оспоренных прав. Доступность суда может быть достигнута двумя взаимообусловленными способами: во-первых, недопущением создания препятствий для реализации права на суд; во-вторых, совершением необходимых действий для создания условий, облегчающих доступ к судебной защите.

Таким образом можно сделать вывод о том, что в результате следует сказать в настоящее время правосудие в нашей стране не в полной мере подчинено принципу доступности, и доступность правосудия зависит от многих факторов: организационных, финансовых, образовательных, процессуальных и др. Для решения данной проблемы необходимы принятие мер социально-экономического характера – снижение неравенства в обществе, повышение качества образования в целом, и в первую очередь – юридического; внедрение информационных технологий; развитие системы бесплатной юридической помощи; обеспечение судебной системы квалифицированными кадрами и некоторые другие.

Список литературы

1. Анишина В. И. Правосудие в современном мире: монография / под ред. В. М. Лебедева, Т. Я. Хабриевой. Москва: Норма, 2012. 234 с.
2. Приходько И. А. Доступность правосудия в арбитражном и гражданском процессе: основные проблемы. СПб: СПбГУ, 2015. 13 с.
3. Статистический отчет за 2017 год // Официальный сайт Управления судебного Департамента г. Севастополя [Электронный ресурс]. Режим доступа: <http://usd.sev.sudrf.ru/modules.php?name=stat&id=16>.
4. Теория государства и права / под ред. С. С. Алексеева. Москва: Норма, 2018. 335 с.
5. Численность населения с денежными доходами ниже величины прожиточного минимума // Официальный сайт Федеральной службы государственной статистики [Электронный ресурс]. Режим доступа: http://www.gks.ru/free_doc/new_site/population/urov/urov_51kv.htm.

Vladimir S. Kolmykov

Student

Institute of Economics and Law (branch)

«Academy of Labor and Social Relations»

¹ Федеральный конституционный закон «О внесении изменений и дополнений в Федеральный конституционный закон «Об арбитражных судах в Российской Федерации» 04.07.2003 г. № 4 ФКЗ //СЗ РФ. – 2003. – № 27 (ч. 1). – Ст. 2699.

(Russia, Sevastopol)
vovchik.zenit@mail.ru

PROBLEMS OF IMPLEMENTATION OF THE PRINCIPLE OF ACCESSIBILITY OF ELECTRONIC JUSTICE IN THE CIVIL PROCESS

Abstract: Defining the range of problems that are an obstacle to the implementation of the principle of accessibility of e-justice in civil proceedings, and the development of ways to solve them.

Keywords: principles, rights, accessibility, justice, judicial, protection.

Костомаров Кирилл Валерьевич

Кандидат юридических наук, доцент,

доцент кафедры уголовно-правовых дисциплин

Уральский институт управления – филиал РАНХиГС при Президенте РФ

(г. Екатеринбург)

k.v.kostomarov@gmail.com

НЕКОТОРЫЕ ОСОБЕННОСТИ ФИКСАЦИИ ДОКАЗАТЕЛЬСТВ ПРИ РАССЛЕДОВАНИИ НЕЗАКОННОГО ДОСТУПА К КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Аннотация: Статья предоставляет ключевые рекомендации по фиксации доказательственной информации при расследовании незаконного доступа к компьютерной информации. Акцент сделан на основных этапах изъятия и фиксации, где возможно изменение, искажение или потеря доказательственной информации в силу её цифровой природы. Обозначены риски несоответствия технического уровня специалистов при фиксации доказательственной информации.

Ключевые слова: компьютерная информация, фиксация доказательств, незаконный доступ к компьютерной информации, специалисты в сфере компьютерной информации, этапы расследования, риски утраты доказательственной информации.

Одним из самых распространенных преступлений в сфере компьютерной информации является неправомерный доступ к компьютерной информации (статья 272 УК РФ). Число таких преступлений в 2016 году составило 994, в 2017 году составило 1079 преступлений, а за 1-ое полугодие 2018 года уже было зарегистрировано 827 таких преступлений. Раскрыто при этом в 2016 году было 529 преступлений (53% от общего числа), в 2017 году 341 (31,6% от общего числа), а в 1-ой половине 2018 года было раскрыто всего 173 преступлений (20,9% от общего числа)¹. Процент раскрытия рассматриваемого вида преступлений недостаточно высок, количество преступлений увеличивается, а количество расследованных преступлений имеет тенденцию к уменьшению в связи с постоянно увеличивающейся технической сложностью механизмов их совершения.

Исходя из обозначенной статистики можно предположить, что существующая в настоящее время методика расследования незаконного доступа к компьютерной информации недостаточно совершенна. Один из важнейших этапов в методике расследования данной категории дел является фиксация доказательственной информации.

Существуют ведомственные методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации, где кратко освещается на какие моменты необходимо обращать внимание при возбуждении и расследовании уголовного дела.

Так, согласно обозначенным рекомендациям, в направляемых для возбуждения уголовного дела материалах должны содержаться: протоколы перехвата и регистрации информации электронной почты лиц, причастных к преступлению, протоколы (акты) изъятия компьютерной техники (машинных носителей) или отражение такого изъятия в протоколах оперативно-розыскных мероприятий, бумажные распечатки информации с изъятых машинных носителей информации и информации, находившейся на жестком

¹ Киберпреступлений становится все больше, однако их раскрываемость уменьшается [Электронный ресурс] / Адвокатская газета. Орган Федеральной палаты адвокатов РФ. Режим доступа: <https://www.advgazeta.ru/novosti/kiberprestupleniy-stanovitsya-vse-bolshe-odnako-ikh-raskryvaemost-umenshaetsya/> (дата обращения 08.05.2019)

диске переносного компьютера подозреваемого, протоколы использования специальных химических средств (химловушек) при фиксации использования компьютерного оборудования в целях неправомерного доступа, краж машинных носителей информации, а также иные документы.¹

При формировании обозначенных материалов дела необходимо учитывать, что в рассматриваемой категории дел для правильной фиксации доказательств требуется уделить особое внимание подготовительному этапу. В противном случае возможно повреждение и даже уничтожение доказательственной базы без возможности восстановления.

Так, перед осмотром места происшествия необходимо пригласить специалистов в сфере компьютерной информации, чтобы снизить угрозу повреждения или уничтожения следов преступлений, необходимо гарантировать неосведомленность собственника компьютера о предстоящем следственном действии, максимально точно определить объекты осмотра, по возможности, определить, какую информацию изучить на месте, а какую изъять для дальнейшего расследования, а также нужно выяснить, подключен ли компьютер к сети, какой установлен пароль; собрать информацию о том, какие средства охраны и обеспечения безопасности компьютерной информации используются, где установлена компьютерная техника... и т.д.²

На месте происшествия необходимо обеспечить допуск к работе с компьютерной техникой только специалистам, изолировать посторонних лиц и лиц, не обладающих соответствующим уровнем компетенции. Затем определить наличие или отсутствие соединения компьютера с иной техникой за пределами осматриваемого помещения. В случае наличия необходимо отключить такое соединение при помощи физического воздействия или с помощью специализированного программного обеспечения для исключения изменения или уничтожения информации. На сегодняшний день уровень технологий перешагнул необходимость физического подключения. Возможности же беспроводного подключения на сегодняшний день настолько широки, что оперативно выявить беспроводное подключение без специальных познаний не всегда возможно, поэтому при работающей компьютерной технике рекомендуется не оставлять без присмотра действующие на ней процессы. Также необходимо определить список активных программ и в случае запуска программы уничтожения или зашифровки информации необходимо их прервать.

При расследовании незаконного доступа к компьютерной информации производится осмотр и фиксация состояния компьютерной техники, выемка документов, фиксирующих состояние информационных носителей в момент вторжения преступника или его программ, а также отображающих последствия вторжения и изъятие следов совершения преступления. Осмотр компьютерной техники и компьютерной информации производят по принципу «от общего к частному». Сначала описывают внешние индивидуальные признаки техники: цвет, размер, тип, вид, название, марка и т.д. Затем переходят к осмотру компьютерной информации.³

Действия следователя зависят также от того, включен или выключен компьютер на начало совершения извлечения информации⁴.

Если компьютер выключен, информацию нужно извлекать следующим образом: первоначально нужно описать местонахождение персонального компьютера (далее – ПК)

¹ Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации // Официальный сайт Генеральной прокуратуры Российской Федерации [Электронный ресурс]. Режим доступа: <https://genproc.gov.ru/documents/nauka/execution/document-104550/> (дата обращения 08.05.2019)

² Балашов Д. Н., Балашов Н. М., Маликов С. В. Криминалистика. М.: ИНФРА-М, 2005.

³ Криминалистическая методика расследования отдельных видов преступлений: учебное пособие в 2-х частях. Ч. 2 / под ред. А. П. Резвана, М. В. Субботиной. М.: ИМЦ ГУК МВД России, 2002. с.84-108.

⁴ Криминалистика. Учебник для вузов / под ред. Р. С. Белкина. М.: Издательство НОРМА.

и его периферийных устройств, описать их соединения друг с другом, перед тем как разъединять какие-либо кабели нужно осуществить фото или видеофиксацию мест их соединения; после соблюдения всех мер предосторожности отключить электропитание и разъединить устройства ПК.

Если компьютер включен, нужно определить программу, которая выполняется на момент осмотра. Дисплей монитора фотографируется, производится фиксация изображения в протоколе, далее следователь останавливает действие программы или ожидает окончания выполняемого действия (к примеру, если идет поиск какой-то информации).

Если для поиска информации используются специализированные программы, это также отражается в протоколе. В случае обнаружения информации дисплей фотографируется еще раз, после чего информация копируется из оперативного запоминающего устройства на съемный носитель.¹

Далее в протоколе отображаются результаты действий следователя, реакции ПК, отсоединяются сетевые кабели, производится копирование программ и файлов, которые хранятся на винчестере, магнитных носителях и пр., отключается подача электроэнергии в ПК и продолжить действия, предусмотренные состоянием выключенного ПК.

В случае если выясняется, что электронные носители информации не содержат значимой информации «изъятые в ходе досудебного производства, но не признанные вещественными доказательствами предметы, включая электронные носители информации, и документы подлежат возврату лицам, у которых они были изъяты» (ч. 4 ст. 81 УПК РФ).

Так, для примера можно рассмотреть приговор по статье 272 УК РФ. В постановлении Устиновского районного суда г. Ижевска Удмуртской Республики по делу № 1-256/17 от 17 ноября 2017 года указано, что часть вещественных доказательств по уголовному делу (монитор, системный блок, манипуляторная мышь, клавиатура, выданные Плотникову И.С), остаются по принадлежности; а три CD-R диска, содержащие информацию, полученную в ходе оперативно-розыскного мероприятия, продолжают храниться при уголовном деле.

Если факт неправомерного доступа обнаружен, необходимо произвести поиск следов пальцев рук на компьютерных и технических средствах поступления информации, охранных устройствах, клавиатуре, кнопках и т.д.², а также поиск микрочастиц.

Если для производства исследования, необходимо большее количество времени, необходимо изъять компьютерную технику и приобщить в качестве вещественных доказательств. Следователь и специалист обесточивают компьютер, разъединив устройства, запаковывают их, и поиск информации осуществляют непосредственно на рабочем месте эксперта или специалиста³. Если произвести изъятие не представляется возможным, нужно наложить запрет на проникновение в помещение и отключить источник питания.

Методика фиксации доказательств в сфере компьютерной информации является быстро устаревающим направлением, поскольку внедрение информационных технологий идёт быстрыми циклами, а большинство рекомендаций написаны более 3-5 лет назад, при этом современные исследования опираются на те, которые были произведены еще в 2000-х годах. В преступлениях в сфере незаконного доступа к компьютерной информации каждый год придумывается что-то новое опираясь на новые программные и технические наработки. Для того чтобы преступления раскрывались успешно, особенности фиксации

¹ Криминалистика Учебник для вузов / под ред. Р. С. Белкина. М.:Издательство НОРМА.

² Мазуров И. Е. Методика расследования хищений, совершенных с использованием интернет-технологий: дис. ...канд. юрид. наук. Казань, 2017.

³ Волеводз А. Г. Компьютерная информация как объект криминалистического следоведения // Криминалистическая техника: учебник / отв. ред. И. М. Балашов, рук. колл. С. В. Маликов. М.: Юрлитинформ, 2008. С.353.

доказательств в цифровой сфере должны быть на особом контроле в связке с техническими специалистами и постоянным обновлением технических средств и методик их применения

Список литературы

1. Балашов Д. Н., Балашов Н. М., Маликов С. В. Криминалистика. М.: ИНФРА-М, 2005. 503 с.
2. Волеводз А. Г. Компьютерная информация как объект криминалистического следования // Криминалистическая техника: учебник / отв. ред. И. М. Балашов, рук. колл. С. В. Маликов. М.: Юрлитинформ, 2008. 608 с.
3. Киберпреступлений становится все больше, однако их раскрываемость уменьшается [Электронный ресурс] / Адвокатская газета. Орган Федеральной палаты адвокатов РФ. Режим доступа: <https://www.advgazeta.ru/novosti/kiberprestupleniy-stanovitsya-vse-bolshe-odnako-ikh-raskryvaemost-umenshaetsya/>.
4. Криминалистика. Учебник для вузов / под ред. Р. С. Белкина. М.: Издательство НОРМА (Издательская группа НОРМА-ИНФРА - М). 990 с.
5. Криминалистическая методика расследования отдельных видов преступлений: учебное пособие в 2-х частях. Ч. 2 / под ред. А. П. Резвана, М. В. Субботиной. М.: ИМЦ ГУК МВД России, 2002. 232 с.
6. Мазуров И. Е. Методика расследования хищений, совершенных с использованием интернет-технологий: дис. ...канд. юрид. наук. Казань, 2017. 188 с.

Kirill V. Kostomarov

PhD in Law, Associate Professor,
Associate Professor of the Department of Criminal Disciplines,
Ural Institute of Management –Branch of RANEPА
(Russia, Yekaterinburg)
k.v.kostomarov@gmail.com

SOME FEATURES OF FIXING EVIDENCE IN INVESTIGATION OF ILLEGAL ACCESS TO COMPUTER INFORMATION

Abstract: The article provides key recommendations on the recording of evidence in the investigation of unlawful access to computer information. The emphasis is on the main stages of seizure and fixation, where change, distortion or loss of evidentiary information is possible due to its digital nature. The risks of non-compliance of the technical level of specialists when fixing the evidentiary information are indicated.

Keywords: computer information, fixing evidence, illegal access to computer information, computer information specialists, investigation stages, risks of loss of evidentiary information.

Косьяненко Елена Михайловна

Кандидат юридических наук, доцент кафедры предпринимательского права
Уральский государственный юридический университет
(г. Екатеринбург)
ekosyanenko@yandex.ru

ПЕРСПЕКТИВЫ ПРАВОВОГО РЕГУЛИРОВАНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА. ИНТЕЛЛЕКТУАЛЬНО-ПРАВОВОЙ АСПЕКТ

Аннотация: В статье проводится критический анализ творческой составляющей результата интеллектуальной деятельности, созданного искусственным интеллектом. Представляется, что автономность деятельности робота не может служить критерием авторства в понимании интеллектуального права. Понятия креативности, интуиции и творчества в отношении искусственного интеллекта наделяются иными характеристиками, нежели аналогичные понятия в отношении человека. Автором результата деятельности искусственного интеллекта, если результат может быть признан охраноспособным объектом авторского права или права промышленной собственности, могут быть признаны субъекты (люди), вложившие творческий вклад в создание подобного объекта, но не в создание искусственного интеллекта.

Ключевые слова: искусственный интеллект, робот, робототехника, искусственный разум, нейропрограммирование, творческая машина, авторское право.

Не успело российское научно-правовое сообщество бурно обсудить, обособить и закрепить на должном уровне правовой режим отношений, возникающих в так называемой «цифровой среде», как появились новые правоотношения и новые объекты современной действительности, требующие немедленного правового вмешательства с целью контроля и регулирования. Речь пойдет об искусственном интеллекте, робототехнике, нейропрограммировании машин и роботов. Мы предлагаем обсудить эти сложные и зачастую неоднозначно понимаемые в юридической среде термины с точки зрения интеллектуального права.

В последние годы право интеллектуальной собственности привлекает все большее внимание цивилистов. Это связано прежде всего с возрастающей ролью нематериальных объектов (результатов интеллектуальной деятельности и средств индивидуализации) в обычной жизнедеятельности человека. Кроме того, коммерциализация таких объектов способствует не только повышению финансовых рейтингов субъектов предпринимательской деятельности, но и привлечению значительных инвестиций для развития и открытия новых инновационных направлений деятельности в различных отраслях экономики. К таким видам деятельности относятся, в частности: нейротехнологии и создание искусственного интеллекта, системы распределенного реестра (блокчейн), компоненты робототехники и сенсорики, технологии виртуальной и дополненной реальностей и др.

При более детальном взаимодействии субъектов с подобными технологиями закономерно возникают вопросы о защите гражданских прав человека на те охраноспособные результаты, которые выдает машина, обладающая по мнению некоторых определенным искусственным интеллектом.

Отталкиваясь от доктрины и теории интеллектуальных прав, согласно которой автором охраноспособного результата интеллектуальной деятельности может быть только человек (гражданин), творческим трудом которого он создан, предлагаем подробнее рассмотреть два основных аспекта: 1) может ли робот выступать субъектом авторских прав в смысле *творческой составляющей объекта, созданного искусственным*

интеллектом; 2) если нет, то кто будет выступать *автором результата деятельности искусственного интеллекта, если результат может быть признан охраноспособным объектом* авторского права или права промышленной собственности?

Мы сознательно не останавливаемся на появлении в социальной и юридической среде термина «искусственный интеллект» хотя бы потому, что численный показатель ответов на поисковый запрос в Google, например, на сегодняшний день превышает 45 млн ответов за 0,53 секунды. Поэтому оспаривать применимость данного термина в настоящее время уже поздно.

Итак, в первую очередь следует обратить внимание на общедоступный и общеизвестный источник – википедию (свободную энциклопедию), в которой размещено определение из толкового словаря и под искусственным интеллектом (англ. Artificial intelligence или AI) понимается свойство интеллектуальных систем *выполнять творческие функции*, которые традиционно считаются прерогативой человека, а также наука и технология создания интеллектуальных машин, особенно интеллектуальных компьютерных программ¹.

О каких творческих функциях идет речь? Разве может машина, обученная выполнять алгоритмические расчеты на основании внесенных в ее память данных отклоняться от заложенной программистами схемы и что-то творить?

Или под творчеством в данном случае понимается заявленное в октябре 2015 года и подтвержденное в марте 2016 года «достижение» компьютерной программы AlphaGo, которая выбрала позицию на доске, ранее не используемую, что принесло машине победу над известными профессиональными игроками? Представители компании-разработчика DeepMind (в штате которой работает около 400 ученых и инженеров, 250 из которых являются кандидатами и докторами наук), громко заявили тогда, что необычный ход программы они расценивают как «творчество и интуицию», после чего привлекли к теме искусственного интеллекта (и к своему техническому продукту) внимание общественности (и соответственно увеличили продажи программы и досок для игры в Го в 10 раз)².

Возможно под творчеством искусственного интеллекта понимают способность машины с помощью искусственных нейросетей консолидировать знания из различных отраслей и создавать на основе этого новое знание?

Если обратиться к истории создания искусственного интеллекта, то именно этот факт послужил открытию в 1994 году Стивенем Таллером способностей своей «творческой машины» и представлению ее как субъекта интеллектуальной деятельности, на результат которой в 1998 году был выдан патент № 5 852 815 (США). Однако следует заметить, что С. Таллер в качестве автора и патентообладателя указал только себя³.

Обстоятельный анализ искусственного интеллекта был проведен в докторской диссертации ученым и практиком, судьей арбитражного суда Морхатом П. М., в ходе которого он предложил дополнить статью 2 Федерального закона от 27.07.2006 № 149-ФЗ (ред. от 29.06.2018) «Об информации, информационных технологиях и о защите информации» новым пунктом 21 следующего содержания: «21) искусственный интеллект – автономный комплекс программных или программно-аппаратных средств (юнит) с человеко-компьютерным интерфейсом, представляющий собой виртуальную вычислительную систему или оснащённую средствами “технического” зрения (восприятия воздействий (сигналов) на сенсорные электронные аналоги органов чувств) и

¹ Толковый словарь по искусственному интеллекту / А. Н. Аверкин и др. М.: Радио и связь, 1992. 256 с. Режим доступа: <http://www.raai.org/library/tolk/aivoc.html#L208> (дата обращения: 18.05.2019).

² Выступление CEO DeepMind Демиса Хассабиса на DLD conference // Youtube.com [Электронный ресурс]. Дата обновления: 22.02.2017. Режим доступа: https://www.youtube.com/watch?time_continue=80&v=Ia3PywENxU8 (дата обращения: 18.05.2019).

³ Artificial Intelligence Collides with Patent Law / Firth-Butterfield K., Chae Y., Allgrove B., Kitsara I. White Paper / Center for the Fourth Industrial Revolution. Geneva (Switzerland): World Economic Forum, 2018. С. 5.

средствами непосредственного самостоятельного взаимодействия с физической реальностью (актуаторами) и с цифровой реальностью киберфизическую систему, с программно-технически и математически эмулированными и обеспеченными способностями (возможностями) биоподобных когнитивных и антропоморфно-интеллектуальных *рече-мыслительных действий (функций)*, обучения и самообучения, самоорганизации и самотестирования, *творческой (эвристической) деятельности*, в том числе на основе накопленных и «исторических» данных и данных мониторинга»¹.

Примеры «творческих достижений» машин можно продолжать. Но ни в первом, ни в последующих примерах не будет и не может быть доказательств того, что искусственный интеллект может понимать, осознавать, чувствовать как человек. Машина, обученная формально-логическому исчислению, даже при способности обучаться самой, поглощая новые пласты информации, не сможет выдать результат, если получит задание, выходящее за рамки программных кодов, созданных непосредственно для нее. Иначе говоря, роботы могут выполнять конкретные заданные функции (пылесосить, варить, чистить, рисовать, управлять транспортом, регулировать освещение, анализировать данные медицинских исследований и сопоставлять их между собой, составлять договоры и исковые заявления и т. д.) и добиваться в этих делах высоких результатов, в первую очередь за счет скорости обработки материала. Но это не дает нам оснований утверждать, что робот может мыслить и творить! Рисовать рисунок по заданным автором программы характеристикам может робот, а создавать произведение искусства, вдохновляясь окружающими людьми, событиями, природой, маленькими деталями и фантазиями, пропуская их через свое мировоззрение и миропонимание может только человек.

Также позволим себе не согласиться с высказываниями И. В. Понкина и А. И. Редькиной о том, что под искусственным интеллектом понимается «сложная кибернетическая компьютерно-программно-аппаратная система, *обладающая свойствами субъективности*»². Ни о какой субъективности машины речи быть не может.

В настоящее время все чаще звучат фразы, аналогичные высказанной профессором Глебовым И. Н.: «... уже сейчас *соревноваться с роботами на равных* людям становится все труднее, а может быть это выше их сил. И это юридическая реальность, с которой должно считаться общество и его законодатели»³.

Напрашивается вопрос: а почему автор решил, что мы соревнуемся на равных? Зачем и кому нужны эти соревнования? Мы не должны опускаться на одну ступень с искусственным интеллектом. Мозг человека решая однотипную задачу (например, играя в шахматы) одновременно выполняет большое количество параллельных немаловажных и сложных задач, обеспечивая работу внутренних органов, сообщая сигналы нервным клеткам и конечностям, получая и анализируя информацию, поступающую из внешних раздражителей через слух, зрение, обоняние и т. д. Машина же (робот), выполняющая однотипную задачу по алгоритму, встроенному в эту машину человеком, не отвлекается на другие задачи. Более того, вряд ли человеческий разум способен снабдить машину всем перечнем задач, которые выполняет наш мозг. Поэтому даже самая сложная машина будет примитивна в сравнении с человеческим мозгом и человеком. И равных соревнований быть не может.

Таким образом, любые суждения о творческой составляющей искусственного интеллекта, а тем более о правосубъектности искусственного интеллекта, представляются

¹ Морхат П. М. Правосубъектность искусственного интеллекта в сфере права интеллектуальной собственности: гражданско-правовые проблемы: дис.... д-ра. юрид. наук. М., 2018. С. 41.

² Понкин И. В., Редькина А. И. Искусственный интеллект с точки зрения права // Вестник Российского университета дружбы народов. Сер.: Юридические науки. 2018. Т. 22. N 1. С. 92.

³ Глебов И. Н. Искусственный юридический разум // Гуманитарное право [Электронный ресурс]. Дата обновления: 01.01.2018. Режим доступа: <https://humanlaw.ru/9-article/26-artificial-intelligence.html> (дата обращения: 19.05.2019)

нам необоснованными, а, следовательно, робот не может быть ни субъектом, ни автором результата интеллектуальной деятельности, согласно нормам гражданского кодекса РФ.

Остается ответить на второй вопрос: кто в таком случае будет признаваться автором охраноспособного результата, полученного от робота? И соответственно кто будет иметь исключительное право на этот результат и нести ответственность за данный результат?

Однозначного ответа на сегодняшний момент нет. Готовы согласиться с Морхатом П. М., предлагающим универсальный вариант, когда «права на результат интеллектуальной деятельности, созданный творческим трудом гражданина, внесшего существенный личный творческий вклад в создание такого результата, при использовании технологий искусственного интеллекта, обеспечивших техническое или информационно-консультационное содействие или помощь, принадлежат этому гражданину.

Права на результат интеллектуальной деятельности, созданный комплексом программных и программно-аппаратных средств искусственного интеллекта автономно, то есть в условиях отсутствия существенного личного творческого вклада человека, принадлежат:

- 1) производителю этого комплекса;
- 2) в случае заключения производителем комплекса программно-аппаратных средств искусственного интеллекта, имеющим на него права, соответствующего лицензионного договора на использование указанного комплекса или его возможностей с физическим или юридическим лицом – лицензиату по указанному договору.

В случае предоставления производителем комплекса искусственного интеллекта, имеющим на него права, открытой лицензии на использование указанного комплекса или его возможностей, в смысле статей 1286.1, 1368 и последнего абзаца пункта 1 статьи 1259 гражданского кодекса, – гражданину, личный творческий вклад которого имел существенное значение как основа для создания этого результата интеллектуальной деятельности, или, при отсутствии такового, переходят в общественное достояние»¹.

Также отвечая на этот вопрос позволим себе обратиться к европейскому опыту. Ещё в 2015 г. в Европейском Парламенте была создана рабочая группа по правовым вопросам, связанным с развитием робототехники и искусственного интеллекта в ЕС. Результатом работы данной рабочей группы стал документ рекомендательного типа «Резолюция Европейского Парламента от 16.02. 2017 г. «Нормы гражданского права о робототехнике»². В ней дается ряд рекомендаций Европейской Комиссии для возможных действий, причём не только касательно норм гражданского права, но и этических аспектов робототехники. Предлагается создать систему регистрации продвинутых роботов, которая управлялась бы Агентством ЕС по робототехнике и искусственному интеллекту. Данное агентство также предоставляло бы техническую, этическую и регулятивную экспертизу по робототехнике. Что касается ответственности, предлагаются два варианта: либо объективная ответственность (не требующая вины), либо подход риск-менеджмента (ответственность лица, которое могло минимизировать риски). Ответственность должна быть пропорциональной реальному уровню указаний, которые отдаются роботу и уровню его автономности. Правила ответственности могут быть дополнены обязательным страхованием для пользователей роботов, и компенсационным фондом для выплаты компенсации в случае отсутствия страхового полиса, покрывающего риск.

В нашей стране необходимо создать подобный орган и возложить на него законодательную и этическую экспертизу искусственного интеллекта. Особенно важно урегулировать вопросы смарт-контрактов, ответственности за военные автономные

¹ Морхат П. М. Правосубъектность искусственного интеллекта в сфере права интеллектуальной собственности: гражданско-правовые проблемы: дис.... д-ра. юрид. наук. М., 2018.

² Resolution and Charter EU 2015/2013 INL P8_TA –PROV (2017)0051 [Резолюция Европарламента от 16 февраля 2017 года 2015/2013(INL) P8_TA-PROV(2017)0051] / пер. Незнамова А. В., Ивановой М. Режим доступа: URL: http://robopravo.ru/riezoliutsiia_ies (дата обращения: 19.05.2019).

системы вооружений и беспилотные транспортные средства (как наземные, так и воздушные), управляемые искусственным интеллектом.

Список литературы

1. Artificial Intelligence Collides with Patent Law / Firth-Butterfield K., Chae Y., Allgrove B., Kitsara I. White Paper / Center for the Fourth Industrial Revolution. Geneva (Switzerland): World Economic Forum, 2018. 23 p.
2. Resolution and Charter EU 2015/2013 INL P8_TA –PROV (2017)0051 [Резолюция Европарламента от 16 февраля 2017 года 2015/2013(INL) P8_TA-PROV(2017)0051] / пер. Незнамова А. В., Ивановой М. Режим доступа: URL: http://robopravo.ru/riezoliutsiia_ies.
3. Глебов И. Н. Искусственный юридический разум // Гуманитарное право [Электронный ресурс]. Дата обновления: 01.01.2018. Режим доступа: <https://humanlaw.ru/9-article/26-artificial-intelligence>.
4. Морхат П. М. Правосубъектность искусственного интеллекта в сфере права интеллектуальной собственности: гражданско-правовые проблемы: дис.... д-ра. юрид. наук. М., 2018
5. Понкин И. В., Редькина А. И. Искусственный интеллект с точки зрения права // Вестник Российского университета дружбы народов. Сер.: Юридические науки. 2018. Т. 22. N 1. С. 91 - 109.
6. Толковый словарь по искусственному интеллекту / А. Н. Аверкин и др. М.: Радио и связь, 1992. 256 с. Режим доступа: <http://www.raai.org/library/tolk/aivoc.html#L208>.

Kosyanenko Elena Mikhailovna

PhD in Law, Associate Professor of the of the Entrepreneurial Law Department,
Ural State Law University
(Russia, Yekaterinburg)
ekosyanenko@yandex.ru

PROSPECTS FOR THE LEGAL REGULATION OF ARTIFICIAL INTELLIGENCE. INTELLECTUAL LEGAL ASPECT

Abstract: The article analyses the creative component of the result of intellectual activity created by artificial intelligence. It seems that the autonomy of the robot activity cannot serve as a criterion of authorship in the understanding of intellectual law. Notions of creativity, intuition and creativity in relation to artificial intelligence are endowed with different characteristics than similar concepts in relation to man. The author of the result of the activity of artificial intelligence, if the result can be recognized eligible the object of copyright or industrial property rights, can be recognized entities (people) who have invested creative contribution to the creation such an object, but not in the creation of artificial intelligence.

Keywords: artificial intelligence, robot, robotics, neuroprogramming, creative machine, copyright.

Кручинина Надежда Валентиновна

доктор юридических наук, профессор, профессор кафедры криминалистики
Московский государственный юридический университет имени О. Е. Кутафина (МГЮА)
(г. Москва)
Nazi93@rambler.ru

**ЭТИЧЕСКИЕ И ПРАВОВЫЕ ВОПРОСЫ ИСКУССТВЕННОЙ РЕПРОДУКЦИИ
ЧЕЛОВЕКА***

Аннотация: В статье исследуются правовые и этические проблемы, связанные с вспомогательными репродуктивными технологиями. Исследуются термины в этой сфере (гестационный курьер, беременность для других, суррогатное материнство). Предлагаются способы криминалистического обеспечения безопасности процесса искусственной репродукции человека от злоупотреблений.

Ключевые слова: Вспомогательные репродуктивные технологии, гестационный курьер, беременность для других, суррогатное материнство, криминалистическое обеспечение.

Количество случаев использования вспомогательных репродуктивных технологий в России увеличивается с каждым годом, а с ними увеличивается количество этических и правовых вопросов. Эти проблемы рассматриваются многими учеными¹. Хотелось остановиться на отдельных проблемах, возникающих, в сфере вспомогательных репродуктивных технологий.

Во-первых, недостаточная информированность пациентов, обращающихся к вспомогательным репродуктивным технологиям (далее – ВРТ). Применение ВРТ связано с применением довольно узких специальных медицинских знаний, которыми располагают сотрудники медицинской клиники. При этом пациенты оказываются уязвимыми в этом плане, поскольку такими знаниями они не обладают. В связи с этим важной стороной применения ВРТ является надлежащее информирование пациента, психологическая консультация и психологическое тестирование пациентов.

Приходящие в клинику репродукции люди могут находиться в состоянии стресса, депрессии. Поэтому в клинике должна проводиться оценка компетентности каждого пациента, то есть его способность принимать зрелые решения. На основании такой оценки врач должен отказаться либо согласиться проводить программу ВРТ с конкретным пациентом².

Во-вторых, необходимо определиться как именовать женщину, которая готова помочь выносить ребенка. Используются разные термины: гестационный курьер, беременность для других, суррогатное материнство, женщина-контейнер. Это важно, чтобы и не обидеть женщину и в тоже время подготовить ее к тому, что с ребенком придется расстаться.

* Исследование выполнено при финансовой поддержке Российского фонда фундаментальных исследований в рамках научного проекта 18-29-14084 «Криминалистическое обеспечение безопасности процесса искусственной репродукции человека от злоупотреблений и преступлений».

¹ Очирова В. В., Доника А. Д. Вспомогательные репродуктивные технологии: правовые основы и этические последствия // Успехи современного естествознания. 2011. № 8. С. 243; Палий В. В. Репродуктивные права человека как потенциальный объект уголовно- правовой охраны // Уголовное право: стратегия развития в XXI веке: материалы XVI Международной практической конференции. М.: РГ-Пресс, 2019. С. 594; Кручинина Н. В., Пятибратова Н. Д. Расследование преступлений против семьи. М., Проспект, 2019. С. 79.

² Новицкая Т. Е. Социально-этические аспекты применения новейших вспомогательных репродуктивных технологий // Вестник Полесского государственного университета. Серия природоведческих наук. 2015. № 1. С. 22.

В-третьих, решение вопроса об использовании ВРТ в неполных (один родитель) семьях. В Федеральном законе «Об основах охраны здоровья граждан» сказано, что мужчина и женщина, которые состоят либо не состоят в браке, имеют право на применение ВРТ в случае наличия добровольного обоюдного и информированного согласия на осуществление медицинского вмешательства. Это касается пар как состоящих, так и не состоящих в браке. Одиноким мужчинам не может воспользоваться ВРТ.

Практика применения ВРТ является причиной трансформации образа семьи, отношений между партнерами, родительства. В отдельных странах право лиц нетрадиционной ориентации на доступ к ВРТ признается на законодательном уровне, а в других странах такие пары не могут воспользоваться такими технологиями. В нашей стране пара гомосексуальных женщин фактически может завести ребенка при помощи ВРТ, если одна из них представится одинокой женщиной и произвести в клинике внутриматочную инсеминацию либо иную процедуру¹.

В-четвертых, в качестве еще одной этической проблемой, а также негативной стороной суррогатного материнства выступает разрушение семейной идентичности. Ребенок имеет очень тесную связь с женщиной, которая его выносила и родила. При этом возможны ситуации, когда женщина, выступая в качестве суррогатной матери, является родившемуся ребенку родственницей. В данном случае такие значащие для каждого человека понятия как мать, бабушка, тетя смешиваясь. В результате стирания понятий, у ребенка возникает неясность своего происхождения, ему не ясны отношения между членами семьи, что может привести к психологическим проблемам.

При реализации процедуры суррогатного материнства, нельзя также обойти стороной и проблемы, которые могут возникнуть у генетических родителей. Это обусловлено несколькими факторами:

- возникновение страха по причине того, что суррогатная мать может расторгнуть договор или же вовсе исчезнет;
- генетическая мать испытывает стресс от того, что вынашиванием ребенка занимается другая женщина;
- переживания родителей за то, что после рождения, суррогатная мать не захочет давать своего согласия и оставит ребенка в своей семье;
- негативные переживания возможны и в процессе воспитания ребенка.

Также не редки случаи, когда родители подсознательно пытаются искать в своем ребенке сходства с женщиной, которая его выносила и родила. Чаще всего это встречается, когда их ребенок находится в пубертатном периоде².

У суррогатной матери могут возникнуть переживания, сомнения, страх.

Нахождение суррогатной матери в таком состоянии пагубно сказывается не только на беременной женщине, но и негативно влияет на ребенка, которого она носит³. Программа суррогатного материнства является еще и серьезным испытанием для мужа женщины, решившей выносить и родить ребенка. Осознание того факта, что его жена вынашивает чужого ребенка для посторонних лиц, пусть даже и на коммерческой основе, тяжела для восприятия ее мужа и имеет свои негативные психологические последствия. Для супругов – это психологическая травма⁴.

¹ Курленкова А. С. Этические проблемы использования вспомогательных репродуктивных технологий // Медицинская этика. 2014. № 1. С. 76.

² Луценко Е. Л., Цокота В. Р. Адаптационный потенциал женщин, готовящихся стать суррогатными матерями // Психологический журнал. 2013. Т. 34. № 3. С. 18.

³ Кузнецова С. В., Шамаева В. В. Этические проблемы пренатальной психологии в суррогатном материнстве // Философские проблемы биологии и медицины сборник статей. / Московский государственный медико-стоматологический университет им. А.И. Евдокимова, Московское философское общество. 2014. С. 109.

⁴ Кулешова К. В., Творогова Н. Д. Психологические риски для "женщины-контейнера", вынашивающей ребенка // «От истоков к современности» (130 лет организации психологического общества при Московском

Более того его согласие спрашивают только один раз при заключении договора. Согласно ст. 51 СК РФ, мужа уже не спрашивают, когда женщина после родов принимает решение дать или нет согласие на запись в качестве родителей генетических родителей. Такую несправедливую ни с этических, ни с правовых позиций ситуацию следует изменить, зафиксировав на законодательном уровне возможность мужа высказать свою позицию также два раза.

В-пятых, в ходе нашего исследования выявлены разные ситуации, связанные с злоупотреблениями и преступлениями, в сфере искусственной репродукции человека. Это и медицинские услуги, которые зачастую оказываются некачественно, это злоупотребления и превышения должностных полномочий, коррупция, мошенничество, вымогательство и т. д.¹

Задачей криминалистики является разработка эффективных технических, тактических и методических рекомендаций выявления и расследования преступлений против репродуктивных прав человека

Таким образом, на сегодняшний день существует большое количество этических проблем, связанных с использованием вспомогательных репродуктивных технологий. Перечень обозначенных проблем не является исчерпывающим и может быть дополнен еще многими и многими из них.

Список литературы

1. Головащук. А. Правовое регулирование вспомогательных репродуктивных технологий в зарубежных странах // Международный журнал прикладных и фундаментальных исследований. 2016. № 1.
2. Кручинина Н. В., Попов В. П. Выявление злоупотреблений и преступлений, связанных с фальсификацией в сфере вспомогательных репродуктивных технологий // Вестник Университета имени О.Е.Кутафина (МГЮА). 2019. № 3 (55). С.95- 101.
3. Кручинина Н. В., Пятибратова Н. Д. Расследование преступлений против семьи. М., Проспект, 2019.
4. Кузнецова С. В., Шамаева В. В. Этические проблемы пренатальной психологии в суррогатном материнстве // Философские проблемы биологии и медицины сборник статей / Московский государственный медико-стоматологический университет им. А.И. Евдокимова, Московское философское общество. 2014.
5. Кулешова К. В., Творогова Н. Д. Психологические риски для "женщины-контейнера", вынашивающей ребенка // «От истоков к современности» (130 лет организации психологического общества при Московском университете): сборник материалов юбилейной конференции в 5 томах / ответственный редактор Д. Б. Богоявленская. 2015.
6. Курленкова А. С. Этические проблемы использования вспомогательных репродуктивных технологий // Медицинская этика. 2014. № 1.
7. Луценко Е. Л., Цокота В. Р. Адаптационный потенциал женщин, готовящихся стать суррогатными матерями // Психологический журнал. 2013. Т. 34. № 3.
8. Новицкая Т. Е. Социально-этические аспекты применения новейших вспомогательных репродуктивных технологий // Вестник Полесского государственного университета. Серия природоведческих наук. 2015. № 1.

университете): сборник материалов юбилейной конференции в 5 томах / ответственный редактор: Д. Б. Богоявленская. 2015. С. 37.

¹ Кручинина Н. В., Попов В. П. Выявление злоупотреблений и преступлений, связанных с фальсификацией в сфере вспомогательных репродуктивных технологий // Вестник Университета имени О.Е.Кутафина (МГЮА). 2019. № 3 (55). С.95- 101.

9. Очирова В. В., Доника А. Д. Вспомогательные репродуктивные технологии: правовые основы и этические последствия // Успехи современного естествознания. 2011. – № 8.

10. Палий В. В. Репродуктивные права человека как потенциальный объект уголовно- правовой охраны // Уголовное право: стратегия развития в XXI веке: материалы XVI Международной практической конференции. М.: РГ-Пресс, 2019.

Nadezhda V. Kruchinina

Doctor of Law, Professor, Professor of the Department of Criminalistics

Kutafin Moscow State Law University (MSAL)

(Russia, Moscow)

Nazi93@rambler.ru

ETHICAL AND LEGAL ISSUES OF MEDICALLY ASSISTED REPRODUCTION

Abstract: The article examines the ethical and legal problems linked with medical assisted reproductive technologies. Examined also is terminology in this sphere (gestational courier, pregnancy for others, surrogacy) are investigated. The author suggests criminological methods appropriate to assure a medically assisted reproduction from abuse.

Keywords: Assisted reproductive technologies, gestational courier, pregnancy for others, surrogacy, forensic support.

Кучин Иван Васильевич
Ведущий партнер
Центр правовых услуг «Регус»
(г. Екатеринбург)
997k@mail.ru

РЕГУЛИРОВАНИЕ КРИПТОВАЛЮТНЫХ ОБМЕННИКОВ

Аннотация: Основной инструмент для совершения сделок по покупке и продаже криптовалюты – онлайн-обменники в сети интернет. В докладе перечислены законодательные изменения, которые, в случае их реализации, могут усилить доверие клиентов к обменникам благодаря более полному правовому регулированию.

Ключевые слова: криптовалюта, онлайн-обменник, сделки с криптовалютой, оператор обмена цифровых финансовых активов.

Вот уже несколько лет популярность криптовалюты набирает обороты. Всё больше людей интересуется криптовалютой. Некоторые пробуют покупать и продавать её. Сделки по купле-продаже криптовалюты обычно происходят на специальных сайтах в сети интернет – обменниках.

Люди приобретают криптовалюту со следующими целями:

1. Расчётная цель – оплата товаров, работ, услуг.
2. Инвестиционная цель – приобретение криптовалюты для её дальнейшего сохранения и продажи по более выгодному курсу.

Для того, чтобы обменять фиатные деньги (например, рубли, доллары, евро и другие) на криптовалюту используются онлайн- и оффлайн-обменники. В онлайн-обменниках можно обменять безналичные деньги на криптовалюту. В оффлайн-обменнике возможно обменять наличные деньги на криптовалюту, т.е. провести не отслеживаемый обмен. Оффлайн-обменников гораздо меньше, чем онлайн-обменников, и они не известны широкому кругу лиц. Подавляющее большинство операций по обмену безналичных денег на криптовалюты происходит в онлайн-обменниках.

В настоящее время онлайн-обменники находятся вне поля правового контроля со стороны государства. При этом существует законопроект № 419059-7 «О цифровых финансовых активах»¹, согласно которому оператор обмена цифровых финансовых активов – юридическое лицо, совершающее сделки по обмену токенов на рубли или иностранную валюту. Операторами обмена цифровых финансовых активов могут быть только юридические лица, которые созданы в соответствии с законодательством Российской Федерации и осуществляют виды деятельности, указанные в статьях 3, 4, 5 Федерального закона от 22 апреля 1996 г. N 39-ФЗ «О рынке ценных бумаг», или юридические лица, являющиеся организаторами торговли в соответствии с Федеральным законом от 21 ноября 2011 г. N 325-ФЗ «Об организованных торгах».

В настоящее время онлайн-обменниками криптовалюты не соблюдаются или соблюдаются не в полной мере три элемента вышеуказанного определения:

1. Требование к организационно-правовой форме. У подавляющего большинства онлайн-обменников криптовалюты на сайтах отсутствуют сведения об организаторе или владельце. Это связано с минимизацией налоговых расходов.

Обычно при продаже криптовалюты клиентом онлайн-обменника, клиенту перечисляются денежные средства не с расчётного счёта организации, а с личного счёта

¹ Законопроект № 419059-7 «О цифровых финансовых активах». Режим доступа: <https://sozd.duma.gov.ru/bill/419059-7> (дата обращения: 18.05.2019).

физического лица. Так же и при покупке криптовалюты денежные средства перечисляются клиентом не на расчётный счёт юридического лица, а на карту другого физического лица. Зачастую банковские карты физических лиц, с которых приходит оплата за продажу криптовалюты, либо на которые поступают деньги за покупку криптовалюты, принадлежат организаторам криптообменников или их близкому кругу доверенных лиц.

Чаще всего используются банковские карты следующих банков: ВТБ, Сбербанк, Тинькофф. При переводе денег за оплату криптовалюты многие обменники просят указать в комментарии к платежу цель перевода: «личный перевод». Это помогает «очистить» деньги от вероятной налоговой нагрузки.

2. Условия статьи 39 Федерального закона «О рынке ценных бумаг» о лицензировании деятельности профессиональных участников рынка ценных бумаг о наличии лицензии не соблюдаются теми криптообменниками, сайты которых я успел изучить при подготовке настоящей статьи.

3. Требования об организационно-правовой форме юридического лица и наличия соответствующей лицензии, предусмотренные Федеральным законом «Об организованных торгах», организаторами торговли не соблюдаются.

Дополнительно я бы хотел обозначить следующие вопросы правового регулирования деятельности криптовалютных обменников.

Первым я обозначу вопрос сбора и обработка персональных данных. Некоторые, но не все, криптообменники просят прислать:

А) фотографию паспорта;

Б) либо фотографию паспорта на фоне открытой заявки на приобретение криптовалюты;

В) либо фотографию паспорта на фоне лица покупателя криптовалюты;

Г) либо фотографию паспорта на фоне лица покупателя криптовалюты с зажатым в руке листком бумаге, на котором написан номер банковской карты или логин покупателя криптовалюты.

Обычно в описании к полю для прикрепления такой фотографии указано, что это необходимо для того, чтобы оценить принадлежность денежных средств конкретному покупателю криптовалюты и исключить возможность противоправного использования чужой банковской карты.

При этом только в очень редких случаях пользователю обменника предлагается заключить электронное соглашение на сбор, обработку и передачу персональных данных. Также большинство серверов, на которых расположена программная часть криптообменников, в нарушение действующего законодательства Российской Федерации, расположено на территориях других стран.

Поскольку покупатель и продавец криптовалюты чаще всего являются резидентами Российской Федерации, оплата криптовалюты происходит в рублях, и обменники, действующие в русском секторе глобальной информационно-телекоммуникационной сети «Интернет», пользуются русским языком как основным, я считаю, что к данному виду правоотношений должны применяться требования федерального законодательства о персональных данных.

Вторым вопросом я обозначу неопределённость в отношении времени исполнения сделки по приобретению криптовалюты.

Действительно, многие обменники предупреждают, что транзакция криптовалюты на электронный кошелек, либо перевод денег за проданную криптовалюту могут занять длительное время. Но иногда на такие транзакции уходит до двух недель. Иногда это связано с отсутствием у владельцев криптообменника свободных денег на банковских картах либо криптовалют на электронных кошельках.

Считаю, что необходимо на законодательном уровне установить лимиты обеспечения сделок с участием криптовалют – минимальные значения количества

денежных средств на банковских счетах и криптовалют на расчётных кошельках. Также необходимо установить временные границы для исполнения сделок, чтобы потенциальным участникам не приходилось ожидать поступления денег или криптовалюты несколько дней.

Третий вопрос – это страхование деятельности криптообменников.

К сожалению, в настоящее время, регулярно происходит «скам» криптообменников. При «скаме» от участников сделок принимаются денежные средства в качестве оплаты за криптовалюту и/или криптовалюта в течение нескольких дней; под надуманными предложениями ответных транзакций не происходит (например, нехватка криптовалюты, блокировка банковских счетов и др.), а затем сайт-обменник и вовсе прекращает функционировать.

Уверен, что необходимо на законодательном уровне установить обязанность криптообменников по страхованию сделок, чтобы в случае неисполнения сделки по любой причине страховая компания компенсировала клиенту обменника сумму по неисполненным обязательствам криптообменника.

Четвёртый вопрос касается информационно-технической безопасности обменников криптовалюты.

Программное обеспечение, которое используют владельцы обменников криптовалют, имеет разную стоимость и обладает разной степенью защиты от взломов. При взломе могут быть утрачены API-ключи, коды двухфакторной аутентификации и иные данные, с помощью которых становится возможным похитить криптовалюту со счёта. Так, например, в ночь с 08 на 09 мая 2019 года с электронных кошельков криптобиржи Binance было похищено более 7 000 биткоинов¹.

Необходимо на законодательном уровне установить минимальные требования для обеспечения полной информационно-технической безопасности сделок, совершаемых с помощью криптовалютных обменников. Например, использование только защищённого соединения, электронно-цифровой подписи, подтверждения сделки посредством использования системы обмена мгновенными электронными сообщениями и др.

Пятый вопрос – это вопрос использования криптообменников для отмывания денег, полученных преступным путём.

В целях соблюдения норм действующего законодательства о противодействии легализации (отмывания) доходов, полученных преступным путем, необходимо распространить действие соответствующего Федерального закона и на криптообменники.

Шестой вопрос – это установление унифицированного комплекта информации, предоставляемой клиентом криптообменнику для совершения сделки, для физических и юридических лиц.

У обменников нет единообразия по процедуре идентификации участников сделок по обмену криптовалюты. Иногда техническая поддержка онлайн-обменников просит прислать фотографии банковской карточки на фоне открытой заявки на обмен денег на криптовалюту или паспорта владельца банковской карточки, с которой перечисляются денежные средства, а иногда нет. При этом у юридических лиц зачастую отсутствует возможность осуществить приобретения криптовалюты в обменнике посредством оплаты её с расчётного счёта.

Для равного доступа физических и юридических лиц к участию в сделках с криптовалютой необходимо на законодательном уровне установить перечень документов, необходимый для совершения такой сделки.

Таким образом, я считаю, что в целях эффективного регулирования криптообменников, необходимо на законодательном уровне:

¹ Нефёдова М. «Злоумышленники похитили у биржи Binance 41 000 000 долларов» [Электронный ресурс]. 2019. Режим доступа: <https://xakep.ru/2019/05/08/binance-attack/>

1. Осуществлять контроль за соблюдением законодательства о персональных данных.
2. Осуществлять контроль за соблюдением норм действующего законодательства о противодействии легализации (отмыванию) доходов, полученных преступным путем
3. Установить минимальные лимиты по запасам денежных средств и криптовалют.
4. Установить максимальную продолжительность исполнения обменником своих обязанностей по сделке, при несоблюдении которой клиенту обменника должны быть возвращены денежные средства и неустойка за неисполнение обязательства.
5. Установить обязанность по страхованию сделок с криптовалютой.
6. Установить минимальные требования для обеспечения полной информационно-технической безопасности сделок, совершаемых с помощью криптовалютных обменников.
7. Установить унифицированный комплект документов для осуществления сделок с криптовалютой как для физических, так и для юридических лиц.

Список литературы

1. Нефёдова М. «Злоумышленники похитили у биржи Binance 41 000 000 долларов» [Электронный ресурс]. 2019. Режим доступа: <https://xakep.ru/2019/05/08/binance-attack>.

Ivan V. Kuchin

Senior partner

Center of legal services «Regus»

(Russia, Yekaterinburg)

REGULATION OF CRYPTOCURRENCY EXCHANGERS

Abstract: The main tool for making transactions of the purchase and sale of cryptocurrencies is online exchangers in the Internet. The report lists legislative changes which could increase customer confidence in exchangers as a result of more complete legal regulation.

Keywords: cryptocurrency, online exchanger, transactions with cryptocurrency, the operator of the exchange of digital financial assets.

Мазунин Яков Маркиянович

Доктор юридических наук, профессор, Заслуженный юрист Российской Федерации,
профессор кафедры криминалистики
Омская академия Министерства внутренних дел Российской Федерации
(г. Омск)
yakovmazunin@yandex.ru

Сидорова Ксения Сергеевна

Адъюнкт
Омская академия Министерства внутренних дел Российской Федерации
(г. Омск)
k_s159@mail.ru

**ОРГАНИЗАЦИОННЫЕ ОСОБЕННОСТИ ПРОИЗВОДСТВА ДОПРОСА С
ИСПОЛЬЗОВАНИЕМ ВИДЕОКОНФЕРЕНЦ-СВЯЗИ**

Аннотация: В статье рассмотрены некоторые организационные особенности проведения допроса с использованием видеоконференц-связи. Показаны причины, вызывающие необходимость допроса посредством видеоконференц-связи. Рекомендованы способы фиксации хода и результатов допроса посредством видеоконференц-связи.

Ключевые слова: допрос, видеоконференц-связь, поручение, внешняя защита, внутренняя защита, фиксация, протокол.

Вопросы, посвященные производству допроса с использованием видеоконференц-связи, рассмотрены в работах таких ученых как Е. А. Архипова, А. И. Гаевой, Н. С. Диденко, Е. Г. Кравец, П. Г. Смагин, С. А. Сумин, В. Н. Чаплыгин, Н. В. Шувалов и другие¹. Законодательством ряда зарубежных стран (например: УПК Украины (ст. 232), УПК Республики Казахстан (ст. 213) предусмотрена возможность производства допроса посредством видеоконференц-связи на досудебной стадии и нормативно урегулирована процедура его проведения. Как указывает А. Г. Волеводз, «отдел обвинения Министерства юстиции США, Атторнейская служба, Федеральное бюро расследований и иные

¹ Архипова Е. А. Применение видеоконференц-связи в уголовном судопроизводстве России и зарубежных стран // Вестник академии генеральной прокуратуры Российской Федерации. 2011. № 5. С. 45-49; Гаевой А. И. Современные информационно-телекоммуникационные технологии как средство повышения эффективности следственных действий: проблемы и перспективы их использования в уголовном судопроизводстве России // Информационная безопасность регионов. 2007. № 1. С. 66-69; Диденко Н. С. Некоторые особенности использования возможностей сети интернет при производстве отдельных следственных действий // Сборник материалов Всероссийской научно-практической конференции «Инновационные методы и образовательные технологии подготовки сотрудников органов внутренних дел» Ростовского юридического института МВД России. 2017. С. 22-30; Кравец Е. Г., Шувалов Н. В. Дистанционные следственные действия сквозь призму применения специальных знаний // Юридическая наука и правоохранительная практика. 2017. № 1. С. 140-144; Смагин П. Г. К вопросу о возможности дистанционного производства следственных действий // Материалы Всероссийской научно-практической конференции «Уголовно-процессуальные и криминалистические проблемы борьбы с преступностью» Орловского юридического института МВД России имени В.В. Лукьянова. 2015. С. 309-314; Сумин С. А. Применение систем видеоконференц-связи при допросе защищаемых территориально удаленных лиц, участвующих в уголовном судопроизводстве на стадиях предварительного и судебного следствия: проблемы реализации и повышение эффективности // Вестник Воронежского института МВД России. 2011. № 3. С. 68-74; Чаплыгина В. Н. Проблемы производства дистанционного допроса в досудебном производстве России // Наука и практика. 2015. № 3. С. 128-130 и др.

следственные органы обладают средствами видеосвязи, зарезервированными для исключительного использования указанными ведомствами»¹.

В соответствии со ст. 218.1 УПК РФ суд, рассматривающий уголовное дело, при необходимости может вынести решение о проведении допроса свидетеля путем использования систем видеоконференц-связи. Представляется, что использование видеоконференц-связи на судебной стадии производства обусловлено обстоятельством, связанным с обеспечением безопасности участников уголовного судопроизводства. При этом мы полагаем, что назрела необходимость разрешения допроса с использованием систем видеоконференц-связи и на стадии предварительного расследования и эта необходимость использования видеоконференц-связи может быть связана не только с этой причиной. Анализ научной литературы и материалов уголовных дел², к числу наиболее распространенных причин востребованности видеоконференц-связи при производстве допроса относятся:

1. Невозможность лица, которого необходимо допросить, прибыть в назначенное место в конкретное время, либо невозможность его прибытия в принципе по уважительным причинам. Причины этому могут быть весьма различны: большое расстояние, требующее значительного времени и материальных затрат для прибытия; состояние здоровья, которое не позволяет совершать переезды и перелеты; другие причины.

2. Причины, связанные с обеспечением безопасности допрашиваемого лица.

3. Причины, связанные с обеспечением разумного срока уголовного судопроизводства.

4. Причины, связанные с нахождением лица в местах лишения свободы или содержанием под стражей.

На основании результатов опроса сотрудников следственных подразделений выявлено, что нередко встречаются ситуации, связанные с тем, что свидетели уклоняются от явки на допрос к следователю в силу того, что находятся в другом населенном пункте и не намерены тратить денежные средства на поездки. В этом случае, как известно, следователем направляется поручение в отдел полиции по месту нахождения лица, которого необходимо допросить, в котором перечисляет вопросы, ответы на которые необходимо выяснить. Данная процедура безусловно тормозит процесс расследования и как верно отмечает Н. Ю. Лебедев, «лицо, которому поручено проведение допроса не знает подробностей совершенного преступления, не знает роли участия допрашиваемого в конкретной следственной ситуации, поэтому вся процедура сводится к тому, что свидетелю зачитываются, перечисленные в поручении вопросы, а в протоколе «сухо» фиксируются его ответы. Процедуру получения таких устных сведений по письменному поручению лишь с натяжкой можно назвать допросом»³.

Кроме этого, практике расследования известны и случаи, когда свидетель неумышленно, например, по состоянию здоровья не может явиться к следователю. Такие ситуации тормозят процесс расследования, что приводит к несвоевременному раскрытию и расследованию преступления.

Исходя из этого, становится возможным констатировать факт того, что допрос с использованием видеоконференц-связи может быть востребован в различных ситуациях, что позволяет без существенных затруднений решить задачи расследования. Соответственно, следователь, принимая решение о проведении допроса с использованием

¹ Волеводз А. Г. Правовые основы взаимной правовой помощи по уголовным делам с использованием видеоконференцсвязи // Военно-юридический вестник приволжского региона. 2003. С. 70-96.

² Лишь в единичных случаях следователями применялись возможности использования видеоконференц-связи при производстве допроса, в то время, как потребность в ней присутствовала более чем в 57% дел.

³ Лебедев Н. Ю. Отсутствие законодательного закрепления процедуры допроса с использованием систем видеоконференц-связи в ходе предварительного расследования – одна из причин возникновения конфликтных ситуаций // Сборник материалов криминалистических чтений. 2015. № 11. С. 37-38.

видеоконференц-связи, может обосновать такое решение необходимым и целесообразным исходя из вышеназванных причин.

В связи с тем, что детально процедура использования видеоконференц-связи при производстве допроса не регламентирована, считаем целесообразным обозначить некоторые тактические особенности, связанные с подготовкой к допросу. Представляется, что, как правило, у следователя возникает вопрос относительно того, каким образом организовать процедуру допроса с использованием видеоконференц-связи, учитывая, что потерпевший или свидетель не могут явиться в кабинет следователя по месту расследования по какой-либо причине. В связи с этим, полагаем, что первоначально необходимо составить поручение в адрес отдела полиции по месту проживания лица в соответствии с п. 4 ч. 2 ст. 38 УПК РФ. Исходя из поставленной задачи о производстве допроса с использованием видеоконференц-связи, представляется целесообразным указать в поручении следующее:

- установление личности человека, которого необходимо допросить;
- принятие мер для обеспечения производства допроса с использованием видеоконференц-связи (техническая составляющая подключения, место проведения следственного действия, присутствие дополнительных участников следственного действия).

Однако перед составлением и направлением поручения в адрес отдела полиции необходимо уточнить, имеется ли техническая возможность в данном отделе полиции для осуществления вызова посредством видеоконференц-связи. Это обусловлено тем, что может иметь место высокая доля вероятности неподготовленности отдела полиции к проведению данного следственного действия. В частности, это может связано с тем, что специально оборудованных помещений для соединения с абонентами посредством видеоконференц-связи в отделах полиции для целей предварительного расследования может и не быть.

В связи с этим, ученые обращают внимание на то, что для проведения следственных действий с использованием видеоконференц-связи необходимо создание специальных помещений и определенного оборудования. Так, по мнению, В. А. Родивилиной «помещения для видеоконференц-связи должны располагать сертифицированным по международным стандартам техническим оснащением, т.е. аудио- и видеооборудованием, телекоммуникационными сетями, позволяющими передавать видеоинформацию в режиме реального времени»¹.

Е. Г. Кравец, Н. В. Шувалов, А. Н. Мартынов также полагают, что для внедрения видеоконференц-связи необходимо учитывать «гарантированную высокоскоростную услугу связи или выделенные каналы связи только для сеансов видеоконференций; оптимальные шумо- и эхопоглощающие особенности помещения, в котором будет установлено оборудование видеоконференц-связи»² и различные другие.

Изложенное позволяет сделать вывод о том, что для технической возможности использования видеоконференц-связи при производстве допроса необходимо создать специальные условия в рамках дислокации определенного органа расследования, что позволит сделать этот процесс более надежным и не повлечь ситуации, связанной с утечкой информации и создаваемыми помехами. Это связано с тем, что сеть «Интернет», к сожалению, не является гарантированным каналом передачи аудио- и видеоданных, который может быть подвержен вирусным атакам.

Вместе с тем, представляется, что необходимо обеспечить как внешнюю, так и внутреннюю защиту канала связи для недопущения перехвата информации, передаваемой

¹ Родивилина В. А. Некоторые вопросы применения видеоконференцсвязи в досудебном производстве // Вестник Иркутского государственного технического университета. 2015. № 2 (97). С. 278-281.

² Кравец Е. Г., Шувалов Н. В., Мартынов А. Н. Перспективы использования видеоконференц-связи при производстве следственных действий на досудебных стадиях уголовного судопроизводства // Юридическая наука и правоохранительная практика. 2017. № 4 (42). С. 175-181.

посредством видеозвонка. При этом внешняя сторона защиты информации связана, прежде всего, с тщательным шифрованием, передаваемой посредством сети «Интернет» информации, а внутренняя с установлением антивирусного программного обеспечения и настройкой безопасности брандмауэра (файервола) (для недопущения захвата сетевого экрана).

Таким образом, при подготовке к проведению допроса с использованием видеоконференц-связи наибольшее значение имеет обеспечение технической составляющей, поскольку она определяет качество передачи информации, и, как следствие – достоверность самого следственного действия.

Полагаем, что отдельного внимания заслуживает вопрос, связанный с фиксацией хода и результатов допроса с использованием видеоконференц-связи. Поскольку законодательством не определено, где должен составляться протокол – по месту нахождения допрашиваемого специально уполномоченным сотрудником, либо по месту нахождения лица, направившего поручение, возникают различные суждения по этому вопросу.

Анализ научной литературы и материалов уголовных дел, позволяет нам сделать вывод о том, что фиксировать данное следственное действие целесообразно проводить по месту расследуемого преступления. Полагаем, что протокол допроса следователю необходимо составлять в электронном виде файлом форматом «DOC» или «DOCX», который после окончания допроса сохраняется и направляется посредством системы электронного документооборота в адрес электронной почты соответствующего отдела полиции, где фактически находится допрашиваемое лицо, после чего, предъявляется всем участникам и подписывается. После этого протокол почтой направляется в адрес отдела полиции по месту расследуемого деяния и подписывается следователем. При необходимости может осуществляться видеозапись допроса с использованием видеоконференц-связи. Возможности современного программного обеспечения для осуществления видео-звонков позволяют в рамках использования имеющейся программы осуществлять его видеозапись.

Изложенное, позволяет сделать вывод о том, что, что такой способ получения доказательственной информации, как производство допроса с использованием видеоконференц-связи, позволит повысить качество и оперативность получения необходимой информации и установить все обстоятельства преступления в кратчайшие сроки.

Список литературы

1. Архипова Е. А. Применение видеоконференц-связи в уголовном судопроизводстве России и зарубежных стран // Вестник академии генеральной прокуратуры Российской Федерации. 2011. № 5. С. 45-49.
2. Волеводз А. Г. Правовые основы взаимной правовой помощи по уголовным делам с использованием видеоконференцсвязи // Военно-юридический вестник приволжского региона. 2003. С. 70-96.
3. Гаевой А. И. Современные информационно-телекоммуникационные технологии как средство повышения эффективности следственных действий: проблемы и перспективы их использования в уголовном судопроизводстве России // Информационная безопасность регионов. 2007. № 1. С. 66-69.
4. Диденко Н. С. Некоторые особенности использования возможностей сети интернет при производстве отдельных следственных действий // Сборник материалов Всероссийской научно-практической конференции «Инновационные методы и образовательные технологии подготовки сотрудников органов внутренних дел». Ростовского юридического института МВД России. Ростов-на-Дону, 2017. С. 22-30.

5. Кравец Е. Г. Дистанционные следственные действия сквозь призму применения специальных знаний / Е. Г. Кравец, Н. В. Шувалов // Юридическая наука и правоохранительная практика. 2017. № 1. С. 140-144.

11. Кравец Е. Г. Перспективы использования видеоконференц-связи при производстве следственных действий на досудебных стадиях уголовного судопроизводства / Е. Г. Кравец, Н. В. Шувалов, А. Н. Мартынов // Юридическая наука и правоохранительная практика. 2017. № 4 (42). С. 175-181.

12. Лебедев Н. Ю. Отсутствие законодательного закрепления процедуры допроса с использованием систем видеоконференц-связи в ходе предварительного расследования – одна из причин возникновения конфликтных ситуаций // Сборник материалов криминалистических чтений. Барнаульского юридического института МВД России. Барнаул. 2015. № 11. С. 37-38.

13. Родивилина В. А. Некоторые вопросы применения видеоконференцсвязи в досудебном производстве // Вестник Иркутского государственного технического университета. 2015. № 2 (97). С. 278-281.

14. Смагин П. Г. К вопросу о возможности дистанционного производства следственных действий // Материалы Всероссийской научно-практической конференции «Уголовно-процессуальные и криминалистические проблемы борьбы с преступностью». Орловского юридического института МВД России имени В. В. Лукьянова. Орел, 2015. С. 309-314.

11. Сумин С. А. Применение систем видеоконференц-связи при допросе защищаемых территориально удаленных лиц, участвующих в уголовном судопроизводстве на стадиях предварительного и судебного следствия: проблемы реализации и повышение эффективности // Вестник Воронежского института МВД России. 2011. № 3. С. 68-74.

12. Чаплыгина В. Н. Проблемы производства дистанционного допроса в досудебном производстве России // Наука и практика. 2015. № 3. С. 128-130.

Yakov M. Mazunin

Doctor of Law, Professor, Honored Lawyer of the Russian Federation,
Professor of the Department of Criminalistics
Omsk Academy of the Ministry of Internal Affairs of the Russian Federation
(Russia, Omsk)
yakovmazunin@yandex.ru

Kseniya S. Sidorova

The Postgraduate Student of the Omsk Academy of the Ministry of Internal Affairs of Russia
(Russia, Omsk)
k_s159@mail.ru

**TACTICAL FEATURES OF THE PRODUCTION OF INTERROGATION USING
VIDEO CONFERENCING**

Abstract: The article discusses some of the organizational features of the interrogation using video conferencing. The reasons for the need to interrogate through video conferencing are shown. Recommended ways to record the progress and results of interrogation through videoconferencing.

Keywords: interrogation, video conferencing, instruction, external protection, internal protection, fixation, protocol.

Никитина Елена Викторовна

Кандидат юридических наук, доцент кафедры уголовного процесса
Уральский государственный юридический университет
(г. Екатеринбург)
nick2210@yandex.ru

НЕКОТОРЫЕ ВОПРОСЫ СОБИРАНИЯ ЭЛЕКТРОННО-ЦИФРОВЫХ ДОКАЗАТЕЛЬСТВ

Аннотация: В статье сделана попытка дать определения понятиям – «электронно-цифровые доказательства» и «электронные носители информации». Исследуются законодательные положения, регулирующие процесс собирания электронно-цифровых доказательств в уголовном судопроизводстве. Акцентируется внимание на тех проблемах, которые возникают на практике в связи с изъятием электронных носителей информации при производстве следственных действий. Дается анализ новой нормы – статьи 164.1 УПК РФ. Делается вывод о том, что конструкция нормы должна быть усовершенствована. Предлагается скорректировать положения статьи 170 УПК РФ с учётом действующей редакции уголовно-процессуального закона.

Ключевые слова: электронно-цифровые доказательства, электронные носители информации, уголовное судопроизводство, следственные действия.

Жизнь современного человека невозможно представить без электронно-цифровых устройств. Соответственно, эти устройства, а также информация, которую они содержат, в ряде случаев могут служить доказательствами по уголовному делу. Что же следует понимать под электронно-цифровыми доказательствами в уголовном судопроизводстве?

Уголовно-процессуальный кодекс РФ не содержит такого термина – «электронно-цифровые доказательства». В статье 84 УПК РФ говорится, что доказательствами по уголовному делу могут быть документы, сведения в которых зафиксированы как в письменном, так и в ином виде. Очевидно, что в последнем случае речь может идти и о документах, содержащих цифровую информацию, представленную на электронном носителе информации. А пункт 5 части 2 статьи 82 УПК РФ одним из видов вещественных доказательств прямо называет электронные носители информации. Как любые доказательства, и те, и другие появляются в уголовном деле в результате производства следственных или иных процессуальных действий (ч.1 ст.86 УПК РФ).

Анализ приведенных выше уголовно-процессуальных норм позволяет прийти к выводу о том, что электронно-цифровые доказательства в уголовном судопроизводстве – это документы или вещественные доказательства, содержащие цифровую информацию, представленную на определенном электронном носителе информации, и полученные в результате следственных или иных процессуальных действий.

Основным способом получения электронно-цифровых доказательств считается изъятие электронных носителей информации в процессе производства следственных действий. Термин «электронные носители информации» появился в УПК РФ в 2012 году¹. Однако законодательных разъяснений относительно того, что понимать под электронными носителями информации, не последовало. В специальной литературе предлагается использовать определение электронных носителей информации, указанное в

¹ О внесении изменений в Уголовно-процессуальный кодекс Российской Федерации: Федер. закон Рос. Федерации от 28 июля 2012 г. № 143-ФЗ: принят Гос. Думой Федер. Собр. Рос. Федерации 3 июля 2012 г.: одобр. Советом Федерации 18 июля 2012 г. // Рос. газ. 2012. 1 августа.

технических стандартах¹. В частности, ГОСТ 2.051-2013 определяет электронный носитель как «материальный носитель, используемый для записи, хранения и воспроизведения информации, обрабатываемой с помощью средств вычислительной техники»². Отталкиваясь от этого определения, большинство исследователей справедливо полагают, что под электронными носителями информации следует понимать любые материальные носители информации в цифровом формате: как внешние, так и являющиеся составной частью электронного устройства³.

Определившись терминологически, можно перейти к законодательным положениям, регулирующим процесс собирания электронно-цифровых доказательств. Первоначально, в 2012 году, законодатель выделил лишь два следственных действия (обыск и выемку), при производстве которых могли быть изъяты электронные носители информации⁴. Статья 182 УПК РФ была дополнена частью 9.1, а статья 183 УПК РФ – частью 3.1. Обе новые нормы регламентировали соответственно обыск и выемку электронных носителей информации. Законодатель посчитал, что изъятие таких носителей информации в ходе обыска и выемки должно производиться в особом процессуальном режиме. Во-первых, электронные носители информации должны изыматься с участием специалиста. Во-вторых, по ходатайству владельца изымаемых электронных носителей или обладателя содержащейся на них информации специалист осуществляет копирование информации на другие электронные носители. В-третьих, такое копирование производится в присутствии понятых. Кроме того, если специалист, участвующий в обыске или выемке, заявит, что копирование информации может повлечь за собой утрату или изменение информации, такое копирование не допускается. Не допускается копирование информации и в том случае, когда это может воспрепятствовать расследованию преступления.

Что означали эти нововведения? Они означали, что особая роль в собирании электронно-цифровых доказательств отводилась специалисту. Без него невозможно было изъять электронные носители информации, произвести с них копирование. Он же мог в ряде случаев сделать заявление о недопустимости копирования.

Как следует из части 1 статьи 58 УПК РФ, специалист – это лицо, обладающее специальными знаниями и привлеченное к участию в процессуальных действиях для содействия в обнаружении, закреплении и изъятии предметов и документов, применении технических средств, для постановки вопросов эксперту при назначении судебной экспертизы, а также для разъяснения суду и сторонам вопросов, входящих в его компетенцию. Применительно к рассматриваемой ситуации специалистом должно быть лицо, обладающее специальными знаниями в области информационных технологий. Чем вызвана необходимость его участия в изъятии электронных носителей информации? Очевидно, законодатель исходил из того, что отсутствие помощи специалиста может повлечь за собой утрату важной доказательственной информации или недостаточно качественное ее копирование.

Однако на практике стали возникать проблемы. Оказалось, что провести следственное действие с участием квалифицированного специалиста довольно затруднительно вследствие высокой степени занятости таких лиц, а также по ряду других

¹ Крюкова Т. С. Некоторые проблемы законодательного регулирования изъятия электронных носителей информации в процессе осуществления следственных действий // Право: история, теория, практика: материалы IV Международной научной конференции (г. Санкт-Петербург, июль 2016 г.). СПб: Свое изд-во, 2016. С. 86.

² ГОСТ 2.051-2013. Межгосударственный стандарт. Единая система конструкторской документации. Электронные документы. Общие положения. М.: Стандартинформ, 2014. С. 2.

³ Першин А. Н. Электронные носители информации как новый источник доказательств по уголовному делу // Уголовный процесс. 2015. № 5. С. 51–52.

⁴ О внесении изменений в Уголовно-процессуальный кодекс Российской Федерации: Федер. закон Рос. Федерации от 28 июля 2012 г. № 143-ФЗ: принят Гос. Думой Федер. Собр. Рос. Федерации 3 июля 2012 г.: одобр. Советом Федерации 18 июля 2012 г. // Рос. газ. 2012. 1 августа.

обстоятельств¹. Кроме того, встал вопрос о целесообразности привлечения специалиста в *каждом* случае изъятия электронных носителей информации. Было высказано мнение о том, что иногда для изъятия конкретных электронных носителей информации помощь специалиста не требуется. Например, вряд ли есть такая необходимость при осуществлении выемки мобильного телефона, цифрового фотоаппарата и т.п.².

Судебная практика шла в основном по пути признания обязательным участия специалиста лишь в том случае, когда проводилось копирование информации. Если копирование не проводилось, отсутствие специалиста не считалось процессуальным нарушением. Однако некоторые суды занимали и противоположную позицию³. Возникла проблема, которую надо было решать на законодательном уровне.

Что касается понятых, то их присутствие при копировании специалистом информации с изымаемых электронных носителей законодатель посчитал необходимым ввиду решения уже чисто процессуальных задач. Понятые призваны были удостоверить факт производства надлежащего копирования информации с изымаемых электронных носителей на другие электронные носители информации. Своей подписью в протоколе следственного действия они подтверждали факт копирования информации и факт передачи электронных носителей информации, содержащих скопированную информацию, законному владельцу изымаемых электронных носителей или обладателю содержащейся на них информации.

Еще одна проблема, существовавшая на тот момент, связана с тем, что законодатель предусмотрел возможность изъятия электронных носителей информации лишь при производстве обыска и выемки. Изъятие таких носителей информации при проведении других следственных действий не предусматривалось, и это обстоятельство также требовало законодательных изменений.

В результате в декабре 2018 года в Уголовно-процессуальном кодексе РФ появилась новая статья, названная «Особенности изъятия электронных носителей информации и копирования с них информации при производстве следственных действий» (ст.164.1 УПК РФ). Одновременно положения части 9.1 статьи 182 и части 3.1 статьи 183 УПК РФ утратили силу⁴. Это означало, что изъятие электронных носителей информации и копирования информации стало возможным при производстве любого следственного действия, а не только при обыске и выемке.

Особый процессуальный режим изъятия этих объектов и копирования информации в целом остался прежним. Отличием от ранее действующих норм стало то, что появилось еще одно ограничение относительно копирования информации – оно не должно производиться, если на электронном носителе содержится информация, полномочиями на хранение и использование которой владелец не обладает, или которая может быть использована для совершения новых преступлений (п.3 ч.1 ст.164.1 УПК РФ). Нововведением стало также то, что следователь при производстве следственного действия получил право по своей инициативе копировать информацию, содержащуюся на электронном носителе информации. При этом в протоколе следственного действия он должен отразить примененные при осуществлении копирования технические средства,

¹ Чернышов В. Н., Лоскутова Е. С. Проблемы собирания и использования цифровых доказательств // Социально-экономические явления и процессы. 2017. Т.12. № 5. С. 201.

² Старичков М. В. Вопросы использования компьютерной информации в качестве доказательств // Известия Тульского гос. университета: Экономические и юридические науки. 2014. Вып. 2. С. 122–123.

³ Крюкова Т. С. Некоторые проблемы законодательного регулирования изъятия электронных носителей информации в процессе осуществления следственных действий // Право: история, теория, практика: материалы IV Международной научной конференции (г. Санкт-Петербург, июль 2016г.). СПб: Свое изд-во, 2016. С. 87.

⁴ О внесении изменений в статьи 76.1 и 145.1 Уголовного кодекса Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации: Федер. закон Рос. Федерации от 27 декабря 2018 г. № 533-ФЗ: принят Гос. Думой Федер. Собр. Рос. Федерации 18 декабря 2018 г.: одобрен Советом Федерации Федер. Собр. Рос. Федерации 21 декабря 2018г. // Рос. газ. 2018. 29 декабря.

порядок их применения, электронные носители информации, к которым эти средства применялись, и полученные результаты. Электронные носители информации, содержащие скопированную информацию, должны прилагаться к протоколу (ч.3 ст.164.1 УПК РФ).

Таким образом, законодатель решил проблему, связанную с ограниченным кругом следственных действий, при производстве которых было возможно изъятия электронных носителей информации. Однако разъяснений по поводу обязательного или необязательного (в ряде случаев) участия специалиста при осуществлении изъятия электронным носителей информации в законе не дается.

Кроме того, сама конструкция статьи 164.1 УПК РФ вызывает ряд вопросов. Начинается статья с запрета изъятия электронных носителей информации по уголовным делам отдельных категорий. Речь идет о некоторых преступлениях, совершенных в сфере предпринимательской или экономической деятельности (ч.4.1 ст.164 УПК РФ). Здесь же перечисляются случаи, являющиеся исключением из этого правила. Часть 2 статьи 164.1 УПК РФ регулирует процессуальный порядок изъятия электронных носителей информации и осуществления копирования с них информации при производстве следственных действий. А часть 3 указанной статьи говорит о праве следователя в ходе следственного действия осуществлять копирование информации, содержащейся на электронном носителе.

При таком построении процессуальной нормы трудно уловить суть закона. А суть, вероятно, сводится к тому, что следователь при производстве следственных действий вправе изымать электронные носители информации, содержащие важную для уголовного дела информацию. Это положение и должно быть отражено в части 1 статьи 164.1 УПК РФ. Далее должен быть указан особый процессуальный порядок изъятия таких электронных носителей. При этом четко должно быть определено, что копирование информации с электронных носителей может быть произведено как по ходатайству законного владельца изымаемых электронных носителей информации (или обладателя содержащейся на них информации), так и без такого ходатайства. В первом случае копирование производится специалистом, участвующим в следственном действии, в присутствии понятых. А во втором случае решение о копировании информации следователь принимает по своей инициативе и может произвести его без привлечения специалиста и понятых. Хотя следует оговориться, что пока трудно судить, действительно ли это имел в виду законодатель, делегируя следователю право осуществлять копирование информации (ч.3 ст.164.1 УПК РФ), или что-то другое. Что касается случаев, когда изъятие электронных носителей информации не допускается, о них, очевидно, следовало сказать в конце. И там же оговорить исключения из этого правила.

Кроме того, хотелось бы обратить внимание еще на один момент. Как уже говорилось, требования закона относительно участия понятых при копировании информации по ходатайству законного владельца изымаемых электронных носителей или обладателя содержащейся на них информации не изменились (ч.2 ст.164.1 УПК РФ). Однако часть 9.1 статьи 182 и часть 3.1 статьи 183 УПК РФ утратили силу в связи с принятием Федерального закона от 27 декабря 2018 года [4]. А положения статьи 170 УПК РФ, регулирующие участие понятых при производстве следственных действий, остались прежними. Там до сих пор фигурирует часть 3.1 статьи 183 УПК РФ, и отсутствует какое-либо упоминание о части 2 статьи 164.1 УПК РФ. Думается, указанные нормы также должны быть скорректированы.

Безусловно, проблемы, связанные с собиранием электронно-цифровых доказательств, пока остаются. Но это не означает, что они не могут быть решены.

Список литературы

1. Крюкова Т. С. Некоторые проблемы законодательного регулирования изъятия электронных носителей информации в процессе осуществления следственных действий //

Право: история, теория, практика: материалы IV Международной научной конференции (г. Санкт-Петербург, июль 2016 г.). СПб: Свое изд-во, 2016. С. 86-88.

2. Першин А. Н. Электронные носители информации как новый источник доказательств по уголовному делу // Уголовный процесс. 2015. № 5. С. 48-54.

3. Старичков М. В. Вопросы использования компьютерной информации в качестве доказательств // Известия Тульского гос. университета: Экономические и юридические науки. 2014. Вып. 2. С. 119-125.

4. Чернышов В. Н., Лоскутова Е. С. Проблемы собирания и использования цифровых доказательств // Социально-экономические явления и процессы. 2017. Т.12. № 5. С. 199-203.

Elena V. Nikitina

PhD in Law, Associate Professor of the Department of Criminal Procedure
Ural State Law University
(Russia, Yekaterinburg)
nick2210@yandex.ru

SOME QUESTIONS OF COLLECTING ELECTRONIC DIGITAL EVIDENCE

Abstract: The article attempts to define the concepts of «electronic digital evidence» and «electronic data carriers». The legal provisions governing the process of collecting electronic digital evidence in criminal proceedings are examined. Attention is focused on the problems that arise in practice in connection with the seizure of electronic media during investigative actions. An analysis of the new standard is given – Article 164.1 of the Code of Criminal Procedure of the Russian Federation. It is concluded that the design of the norm should be improved. It is proposed to adjust the provisions of Article 170 of the Code of Criminal Procedure of the Russian Federation taking into account the current edition of the criminal procedure law.

Keywords: electronic digital evidence, electronic data carriers, criminal proceedings, investigative actions.

Олейникова Юлия Олеговна

Студент

Иркутский юридический институт (филиал)
Университета прокуратуры Российской Федерации
(г. Иркутск)
yulia-oleinikov@mail.ru

К ВОПРОСУ ОБ ИСПОЛЬЗОВАНИИ ГЕНОМНОЙ ИНФОРМАЦИИ ПРИ РАСКРЫТИИ ПРЕСТУПЛЕНИЙ

Аннотация: В статье рассматриваются основные аспекты осуществления обязательной геномной регистрации в России. Автор обращается к зарубежному опыту и оценивает его возможную имплементацию в отечественную практику получения геномной информации. Делается акцент на необходимости усовершенствования механизмов охраны геномной информации. Анализируются дальнейшие перспективы развития института геномной регистрации в Российской Федерации. Делается вывод о неоднозначности использования геномной информации при раскрытии преступлений.

Ключевые слова: геномная информация, геномная регистрация, идентификация, биологический материал.

С развитием науки появились новые возможности регистрации и идентификации мирового населения. Один из них – геномная регистрация, которая представляет собой процесс изъятия уполномоченными органами биологических материалов человека с целью последующего получения геномной информации. Безусловно, подобный метод может быть весьма полезным и надежным для решения задач криминалистики: «Стремительное развитие нано- и биотехнологий ставит вопрос о возможности применения методов молекулярной биологии в криминалистике и судебной медицине»¹.

К настоящему моменту на базе Интерпола сформирована обширная база данных ДНК, пользование которой осуществляют 84 государства². Первенство в использовании метода ДНК-анализа для раскрытия преступлений принадлежит Великобритании. По состоянию на июль 2018 года Национальная база данных ДНК Великобритании (NDNAD) содержала 6,024,032 генетических профилей лиц (что составляет чуть более 9% от численности населения Великобритании) и 555,362 генетических профилей, изъятых с мест преступлений³. Для сравнения, по данным МВД России, на период января 2017 года в ФБДГИ (Федеральной базе данных геномной информации) содержалась информация 0,14% населения Российской Федерации⁴.

Дефиниция понятия «геномная информация» предусмотрена в п. 3 ст. 1 Федерального закона от 03.12.2008 № 242-ФЗ «О государственной геномной регистрации в Российской Федерации»⁵ (далее – закон), согласно которому под ней подразумеваются «персональные данные, включающие кодированную информацию об определенных

1 Бородулин В. Б., Родионова М. П. Применение молекулярно-генетических методов в раскрытии преступлений // Информационная безопасность регионов. 2010. № 2. С. 116.

2 Connecting police for a safer world [Электронный ресурс]. Режим доступа: <http://www.interpol.int/INTERPOL-expertise/Forensics/DNA> (05.05.2019).

3 National DNA Database Strategy Board Annual Report 2016/17 [Электронный ресурс]. Режим доступа: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/724596/040718_new_CCS0518718592_National_DNA_Database_Strategy_Board_AR_2016-17_updates_NEW.pdf (05.05.2019).

4 Гостев А. А. По биологическим следам: интервью от 13.01.2017 // Объединенная редакция МВД России. Режим доступа: <http://www.ormvd.ru/interview/po-biologicheskim-sledam/> (05.05.2019).

5 О государственной геномной регистрации в Российской Федерации: Федер. закон от 03 дек. 2008 г. № 242-ФЗ: в ред. от 17.12.2009 // Собр. законодательства Рос. Федерации. 2008. № 49. Ст. 5740.

фрагментах дезоксирибонуклеиновой кислоты физического лица или неопознанного трупа, не характеризующих их физиологические особенности». При этом под государственной геномной регистрацией необходимо понимать «деятельность, осуществляемую указанными в Федеральном законе государственными органами и учреждениями по получению, учету, хранению, использованию, передаче и уничтожению биологического материала и обработке геномной информации» (п. 1 ст. 1).

Необходимо отметить, что с момента принятия указанного закона и до настоящего времени в его адрес было высказано немало критических замечаний, связанных, в первую очередь, с узким кругом лиц, подлежащих обязательной государственной геномной регистрации. Так, в соответствии со ст. 7 закона, геномной регистрации в обязательном порядке подлежат лица, осужденные и отбывающие наказание в виде лишения свободы за совершение тяжких или особо тяжких преступлений, а также всех категорий преступлений против половой неприкосновенности и половой свободы личности; неустановленные лица, биологический материал которых изъят в ходе производства следственных действий, а также неопознанные трупы. По мнению исследователей, данный перечень подлежит расширению. Подобная позиция основана на следственной практике, а также на анализе зарубежного опыта. Например, в Великобритании обязательной геномной регистрации подлежат, в том числе, лица, совершившие административные правонарушения. А в базе данных ДНК Исландии содержатся генотипы всего населения государства. Такой подход нашел отклик в отечественной доктрине: «Тотальное проведение геномной регистрации будет служить сдерживающим фактором для людей, склонных к совершению преступлений, а, следовательно, иметь профилактическое значение, позитивно влиять на криминогенную ситуацию в стране»¹.

Применительно к российскому законодательству, предлагается, например, «обязательный забор крови у новорожденных детей; всех женщин (в том числе беременных) находящихся в возрасте до 45 лет, рождающихся и обслуживающихся в медицинских учреждениях РФ, проходящих плановые и внеплановые осмотры в медицинских учреждениях»². Также для расширения возможностей идентификации, ряд ученых призывает к осуществлению государственной геномной регистрации родственников людей, пропавших без вести, а также самих безвестно пропавших граждан^{3,4}. Кроме этого высказывается предположение о целесообразности обязательной геномной регистрации лиц, «представляющих оперативный интерес, но в отношении которых нет достаточных данных для решения вопроса о возбуждении уголовного дела. В соответствии с ФЗ «Об оперативно-розыскной деятельности» это лица, подготавливающие, совершающие или совершившие преступления. Причем, биологические образцы данных лиц, подлежащие обязательной постановке на учет, могут быть получены как гласным, так и негласным путем»⁵. В любом случае, большинство исследователей уверены, что «расширение круга лиц, подлежащих учёту, в значительной

¹ Старченко А. В. Современные возможности использования метода генотипоскопии в биологической экспертизе при расследовании преступлений // Известия Тульского государственного университета. 2015. № 2-2. С.94.

² Лукомская А. С. К вопросу о государственной геномной регистрации // Вестник Оренбургского государственного университета. 2012. – № 3 (139). С. 93.

³ Исмаилов Ч. М. Безвестное исчезновение как признак преступления и как повод уголовно-процессуальной проверки // Российский следователь. 2014. № 2. С. 24.

⁴ Надоненко О. Н. Особенности реализации федеральной программы геномной регистрации // Юридический мир. 2015. № 1. С. 33.

⁵ Кубитович С. Н. Биологическая экспертиза и учет геномной информации в России // Вестник экономической безопасности. Юридические науки. 2018. № 1. С. 75-76.

степени будет способствовать решению задачи раскрытия преступлений»¹. В связи с этим предвидится скорейшее введение системы так называемых генетических паспортов.

Однако такая позиция не может считаться однозначной. Сама по себе геномная регистрация может представлять опасность для государства, общества и человека в случае ненадлежащей защиты геномной информации.

Противники геномной регистрации обосновывают свое мнение следующими аргументами. Во-первых, существуют сомнения в достаточном уровне защиты информации о геноме того или иного человека. Геномная информация, как и любая личная информация, охраняется государством в порядке, предусмотренном Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», а также Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации». При этом вероятно, что геномная информация в силу своей специфичности нуждается в обособленном правовом регулировании и повышенной юридической ответственности за ненадлежащее ее хранение. Уровень опасности последствий при возможной «утечке» генетической информации может дифференцироваться от нарушения права человека на неприкосновенность частной жизни и личную тайну (что впоследствии может привести к «генетическому апартеиду» и дискриминации граждан²), до более катастрофических последствий: «Если знать генетический код человека, то при желании можно подобрать ему такую пищу или лекарства, которые просто его уничтожат. Фактически, имея информацию о генетическом коде, представителям той или иной этнической группы можно заблокировать их гены так, что они перестанут рождаться»³.

Во-вторых, не исключена возможность ошибок – как субъективных, так и объективных – в результате экспертизы: «Ошибки могут возникать на каждом из этапов экспертизы – от сбора образцов до вынесения итогового заключения. Совсем несложно перенести ДНК с одного места на другое, смешать пробы и т. д., то есть сфальсифицировать результаты судебного исследования. Причем допущенные ошибки могут быть обращены как во вред, так и в пользу подозреваемого»⁴. При этом справедливо отметить, что от фальсификации не защищено ни одно доказательство, предусмотренное УПК РФ.

Более прагматичный аргумент заключается в отсутствии необходимой материальной базы (в первую очередь, финансовой) для расширения существующей ФБДГИ.

При этом большинство авторов настаивают, что указанные недостатки устранимы, а потому не являются аргументом отказа от формирования геномных баз данных⁵. При этом потребуется обеспечение максимальной защиты ФБДГИ со стороны государства – правовой, организационно-технической и криптографической. Только при увеличении гарантий сохранности геномной информации возможно расширение ФБДГИ для решения задач, предусмотренных законодателем для геномной регистрации.

¹ Жога Е. Ю., Васенин А. Ю., Варченко И. А. Роль государственной геномной регистрации в предупреждении, раскрытии и расследовании преступлений // Гуманитарные, социально-экономические и общественные науки. Государство и право. Юридические науки. 2017. № 6-7. С. 4.

² Сафонов А. А., Курин А. А., Варченко И. А. Закон принят, а нужна ли России геномная регистрация и каковы перспективы ее использования? // Общество и право. Государство и право. Юридические науки. 2009. № 4 (26). – С. 261.

³ Героева А. МВД регистрирует граждан на генетическом уровне // Коммерсантъ. 2007. № 89. Режим доступа: <http://www.kommersant.ru/doc/768636> (05.05.2019).

⁴ Баженова Л. В. Перспективы развития генетической идентификации // Известия Тульского государственного университета. 2016. № 2-3. С. 160.

⁵ Попова Т. В., Сергеева А. Б. Федеральная база данных геномной информации в системе обеспечения баланса частных и публичных интересов в уголовном судопроизводстве // Юридическая наука и правоохранительная практика. 2017. № 1. С. 132–139.

Список литературы

1. Connecting police for a safer world. [Электронный ресурс]. Режим доступа: <http://www.interpol.int/INTERPOL-expertise/Forensics/DNA>.
2. National DNA Database Strategy Board Annual Report 2016/17 [Электронный ресурс]. Режим доступа: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/724596/040718_new_CCS0518718592_National_DNA_Database_Strategy_Board_AR_2016-17_updates_NEW.pdf.
3. Баженова Л. В. Перспективы развития генетической идентификации / Л. В. Баженова // Известия Тульского государственного университета. 2016. № 2-3. С. 155-161.
4. Бородулин В. Б., Родионова М. П. Применение молекулярно-генетических методов в раскрытии преступлений // Информационная безопасность регионов. 2010. № 2. С. 115-120.
5. Героева А. МВД регистрирует граждан на генетическом уровне // Коммерсантъ. 2007. № 89. Режим доступа: <http://www.kommersant.ru/doc/768636>.
6. Гостев А. А. По биологическим следам: интервью от 13.01.2017 // Объединенная редакция МВД России. Режим доступа: <http://www.ormvd.ru/interview/po-biologicheskim-sledam/>.
7. Жога Е. Ю., Васенин А. Ю., Варченко И. А. Роль государственной геномной регистрации в предупреждении, раскрытии и расследовании преступлений / Е. Ю. Жога, А. Ю. Васенин, И. А. Варченко // Гуманитарные, социально-экономические и общественные науки. Государство и право. Юридические науки. 2017. № 6-7. С. 2-8.
8. Исмаилов Ч. М. Безвестное исчезновение как признак преступления и как повод уголовно-процессуальной проверки // Российский следователь. 2014. № 2. С. 21-25.
9. Кубитович С. Н. Биологическая экспертиза и учет геномной информации в России // Вестник экономической безопасности. Юридические науки. 2018. № 1. С. 72-77.
10. Лукомская А. С. К вопросу о государственной геномной регистрации / А. С. Лукомская // Вестник Оренбургского государственного университета. 2012. № 3 (139). С. 92-94.
11. Надоненко О. Н. Особенности реализации федеральной программы геномной регистрации // Юридический мир. 2015. № 1. С. 33-36.
12. Попова Т. В., Сергеева А. Б. Федеральная база данных геномной информации в системе обеспечения баланса частных и публичных интересов в уголовном судопроизводстве // Юридическая наука и правоохранительная практика. 2017. № 1. С. 132-139.
13. Сафонов А. А., Курин А. А., Варченко И. А. Закон принят, а нужна ли России геномная регистрация и каковы перспективы ее использования? // Общество и право. Государство и право. Юридические науки. 2009. № 4 (26). С. 259-262.
14. Старченко А. В. Современные возможности использования метода генотипоскопии в биологической экспертизе при расследовании преступлений // Известия Тульского государственного университета. 2015. № 2-2. С. 93-97.

Yulia O. Oleynikova

Student of Irkutsk Law Institute (branch)
of the University of Prosecutor's Office of the Russian Federation
(Russia, Irkutsk)
yulia-oleinikov@mail.ru

**ON THE ISSUE OF USING GENOMIC INFORMATION FOR DETECTION OF
CRIMES**

Abstract: The article deals with the main aspects of the mandatory genomic registration implementation in Russia. The author turns to foreign experience and assesses its possible implementation in the domestic practice of obtaining genomic information. It is also focused on necessity of improving mechanisms for the protection of genomic information. The study explores and analyses perspectives of development of the genomic registration institute in the Russian Federation. The conclusion is made about the ambiguity of using genomic information in the detection of crimes.

Keywords: genomic information, genomic registration, identification, detection of crimes, biological material.

Пичугов Михаил Сергеевич
Студент Института юстиции
Уральский Государственный Юридический Университет
(г. Екатеринбург)
mpicugov843@gmail.com

ДЕАНОНИМИЗАЦИЯ ПРЕСТУПНИКА, СОВЕРШИВШЕГО ПРЕСТУПЛЕНИЕ В СЕТИ «ИНТЕРНЕТ»

Аннотация: В статье описываются статистика, примеры и способы совершения киберпреступлений, их позиция в общей массе преступлений на данном этапе. Описываются инструменты, с помощью которых киберпреступник скрывает свою личность и замечает следы, и инструменты, которые можно задействовать для раскрытия личности киберпреступника, а точнее инструменты деанонимизации хакера, который пытается избежать наказания путем анонимизации своей личности в сети «Интернет»

Ключевые слова: киберпреступления, киберпреступник, компьютер, прокси-сервер.

Появление компьютеров и международной компьютерной сети Интернет привело к появлению так называемых «компьютерных преступлений». В соответствии со статистическими данными, ежегодно публикуемыми ГИАЦ МВД России, в Российской Федерации за 2017 год зарегистрировано 1883 преступления в сфере компьютерной информации. Если говорить о преступлениях, совершенных с использованием компьютерных и телекоммуникационных технологий, их количество составило 62404. Однако ни первый, ни второй показатель не позволяет увидеть, сколько уголовно-наказуемых деяний совершено лицами, которые подыскивая себе орудия и средства совершения преступлений, посетили заблокированные сайты в сети Интернет. Российское законодательство не относит к категории уголовно-наказуемых такие действия, как посещение запрещенных сайтов.

Вести учет компьютерных преступлений непросто, но общее их число во много раз превышает данные из статистики МВД. Реальное количество киберпреступлений в России минимум в 5 раз больше. Количество взломов почты, например, исчисляется миллионами, а они тоже являются киберпреступлениями, говорит руководитель департамента расследований инцидентов Group-IB (расследование киберпреступлений) Дмитрий Волков. Он сообщает, что попытки хищения денег происходят намного реже, чем взломы почты, но не менее 100 000 в год и часть из них блокируется банками. По данным Group-IB, в 2013 г. киберпреступники заработали в России и СНГ \$2,5 млрд.

В 2014 г. МВД зарегистрировало в России 11 000 компьютерных преступлений. Об этом со ссылкой на заявил начальник Бюро специальных технических мероприятий МВД России Алексей Мошков.

Согласно статистическим данным, в 2017 году число преступлений в сфере информационно-телекоммуникационных технологий увеличилось с 65 949 до 90 587. Их доля от числа всех зарегистрированных в России преступных деяний составляет 4,4% - это почти каждое 20 преступление.

Самыми распространенными киберпреступлениями являются неправомерный доступ к компьютерной информации (статья 272 УК РФ), создание, использование и распространение вредоносных компьютерных программ (статья 273 УК РФ).

При этом на 19,6% уменьшилось количество расследованных преступлений по указанным статьям (с 903 до 726), выросло на 30,5% (с 790 до 1031) число нераскрытых преступлений. Раскрываемость данных преступлений составила 41,3%.

Распространение получили мошеннические действия, совершенные с использованием электронных средств платежа (статья 159.3 УК РФ). Их количество в первом полугодии 2018 г. возросло в 7 раз.

Количество преступлений, совершенных в 2017 году составляет 2 058,5 тыс. Киберпреступления в дальнейшем могут стать самыми проблемными преступлениями в России, потому их количество увеличивается прямо пропорционально развитию компьютеров и интернета, а сложность и не раскрываемость преступлений увеличивается с развитием программного обеспечения. Также киберпреступления опасны еще и тем, что являются одними из самых молодых и видоизменяющихся преступлений.

Также можно отметить недавнее судебное разбирательство с хакерской группировкой под названием «Lurk»

Напомним, что группировку Lurk удалось ликвидировать в ходе совместного расследования программистов «Лаборатории Касперского», ФСБ и МВД РФ. Согласно многостраничному докладу, выпущенному впоследствии специалистами «Касперского», хакеры работали как небольшая компания по разработке программного обеспечения.

Существовали целые «отделы», занимавшиеся разработкой, тестированием или внедрением одноименного трояна Lurk. Отдельное подразделение отвечало за создание юридических лиц, вывод и обналичку похищенных средств через так называемых дропов. Благодаря внедрению трояна на компьютеры российских компаний, хакеры выводили с их счетов сотни миллионов рублей.

Группировка хакеров получила свое название из-за троянской программы Lurk (англ. затаиться). Впервые ее выявили специалисты «Лаборатории Касперского» в 2011 году. Впоследствии именно эксперты антивируса помогли силовикам выйти на след группировки.

В 2011-м троян использовался хакерами для заражения банковских компьютеров. Программа подменяла реквизиты в платежных поручениях и таким образом отправляла денежные переводы на подконтрольные киберпреступникам счета.

С развитием антивирусов и банковского программного обеспечения начал совершенствоваться и Lurk. Следившие за эволюцией трояна специалисты «Касперского» в 2013 году пришли к выводу, что за разными версиями программы стоят одни и те же разработчики.

Согласно многостраничному докладу, выпущенному «Лабораторией Касперского» после арестов членов группировки, хакеры работали как небольшая компания по разработке программного обеспечения. Существовали целые «отделы», занимавшиеся разработкой, тестированием или внедрением Lurk. Отдельное подразделение отвечало за создание юридических лиц, вывод и обналичку похищенных средств через так называемых дропов¹.

Рассмотрим инструменты сокрытия личности киберпреступника.

Сохранение анонимности в компьютерной сети Интернет не следует обязательно рассматривать как нечто противозаконное. Многие пользователи стремятся к анонимности и с этой целью используют вымышленные имена, ники, чужие компьютеры для выхода в сеть. В отдельных случаях меняется MAC-адрес сетевого устройства, IP-адрес компьютера. Делается это по самым разным причинам. Например, ознакомиться с информацией, находящейся на чужом аккаунте, избежать всплывающей рекламы или так называемого «спама» при посещении интернет-магазинов, иных Интернет-ресурсов. Посетители «темного» Интернета пытаются скрыть данные о своей личности с единственной целью – избежать уголовной ответственности за совершаемые ими противозаконные действия. При этом они, помимо вышеперечисленных простейших

¹ Антоненков Д. Они обчищали банки, следили за миллиардерами и читали письма Хиллари Клинтон. История хакеров Lurk. // Новостной портал 66.RU [Электронный ресурс]. Дата обновления: 04.10.2018. Режим доступа: <https://66.ru/news/internet/215767/> (дата обращения: 18.05.2019).

способов, используют и более совершенные способы сохранения анонимности. Речь идет об использовании сервисов-анонимайзеров или сервисов, которые позволяют анонимно посещать интересующие пользователей сайты. Говоря о подобных сервисах можно отметить, что по сути это некие посредники между пользователем и интересующим его ресурсом. Это могут быть прокси-серверы, vpn-сети, браузеры. Рассмотрим подробнее каждый из них. Лица, занимающиеся поиском в компьютерной сети Интернет той или иной информации, нередко обращаются к услугам дополнительных прокси-серверов.

Что касается особенностей работы сервиса-анонимайзера, то он заключается в следующем. Лицо, желающее сохранить в тайне обращение к сайтам, находящимся в «темном» Интернете, заходит на страницу анонимного прокси-сервера. Далее в адресной строке указывает адрес сайта, который он хочет посетить. При этом анонимайзер сам скачивает с сайта информацию (или передает ее на интересующий сайт), а пользователь получает доступ к ней с сервера анонимайзера. Использование такой схемы позволяет пользователю скрыть свои данные, IP-адрес своего компьютера и, таким образом, сохранить анонимность. Но следует отметить, что указанные сведения чаще всего сохраняются на сервере анонимайзера. Лица, желающие сохранить свою анонимность, активно пользуются в последнее время VPN соединением. VPN (Virtual Private Network) – представляет собой виртуальную частную сеть. Пользователь соединяется с провайдером по закрытому каналу (тоннелю), который обеспечивается благодаря зашифрованной передаче данных. Тем самым достигается безопасность соединения, а также и анонимность пользователя. Возникает вопрос: «Сохраняются ли сведения о пользователе на сервере провайдера?» В 2013 году Интернет-ресурсом torrentfreak.com было проведено интересное «исследование». VPN-провайдерам был задан вопрос о том, хранят ли они журналы, позволяющие сопоставить IP-адрес с обратившимся к ним клиентом. В своих ответах провайдеры были категоричны и заявили, что журналы они не хранят, либо хранят их недолго, а установить по ним клиента невозможно.

Еще один способ сохранения анонимности, к которому обращаются, это использование специальных браузеров. Наибольшую популярность среди лиц, стремящихся к сохранению своей анонимности в сети, приобрел TOR Browser, который позволяет выходить в одноименную сеть Tor. Работа сети построена на использовании так называемой «луковой» маршрутизации. Суть ее заключается в использовании системы специальных узлов, которые последовательно шифруют информацию о пользователе и маскируют действующий IP-адрес компьютера. Специальные узлы – это компьютеры и серверы нескольких тысяч пользователей, входящих в единую анонимную сеть. Как правило, соединение пользователя происходит через три случайных узла (входной, промежуточный и выходной). Каждому из указанных узлов неизвестны адреса пользователя и интересующего его ресурса одновременно (иначе говоря, известно только откуда пришли данные и куда их необходимо отправить). Такой способ работы в компьютерной сети Интернет, несмотря на низкую скорость, позволяет с достаточно высокой степенью вероятности сохранить в тайне данные пользователя, обратившегося на какой-либо закрытый сайт.

Резюмируя вышеперечисленное отметим, что киберпреступники могут прибегать к самым различным способам обеспечения анонимности в сети Интернет. Использование ника, вымышленного имени, чужого компьютера, изменение MAC-адреса сетевого устройства, IP-адреса компьютера. Перечисленные способы относительно просты, но оставляют возможность идентифицировать устройство, с которого произошел выход в компьютерную сеть Интернет и посещение того или иного сайта. Вторая группа включает в себя способы, связанные с использованием прокси-серверов, сервисов-анонимайзеров, VPN соединения, специальных браузеров. В этих случаях идентификация устройства, с которого был совершен выход в Интернет, а, в конечном итоге, киберпреступника, посетившего какой-либо заблокированный сайт, становится затруднительной. Здесь следует учитывать, что помимо изменения MAC-адреса сетевого устройства, IP-адреса

компьютера, проблема осложняется следующим обстоятельством. При использовании сервисов-анонимайзеров, VPN соединения, специальных браузеров соответствующие серверы, через которые происходит соединение, довольно часто расположены не на территории Российской Федерации.¹

Использование всех этих средств может предоставить вам анонимность, но не гарантировать, что вас не найдут. Ведь эти средства не делают поиск нереальным, но создают некое препятствие для деанонимизации вас.

Если рассматривать все эти инструменты как способ сокрытия следа киберпреступника, то в каждом из них можно найти недостатки, которые деанонимизируют личность киберпреступника. В совокупности их работа неидеальна и след киберпреступника возможно найти. Прокси-сервер – промежуточный сервер, который находится между пользователем и интересующим его сайтом (ресурсом). Процесс получения необходимой информации происходит следующим образом. Пользователь запрашивает информацию, находящуюся на другом сервере путем обращения к прокси-серверу. Последний, подключившись к указанному серверу, получает информацию. А пользователь забирает ее уже с прокси-сервера в неизменном виде (либо видоизмененную). Работа прокси-сервера представляет собой ширму, за которой сидит человек и перекидывает бумажки через ширму другому человеку, чтобы узнать ответ на свой вопрос, а второй в свою очередь кидает ему бумажку с ответом, при всем этом, ни один, ни второй не знают, кто сидит за ширмой. Анонимизация с помощью прокси-серверов представляет собой создания множество ширм, которые усложняют нахождение человека, который делает запрос, но работа в интернете подразумевает получение и отправку запросов через тот IP-адрес, который выдает провайдер для пользования интернетом. Это так называемый физический IP-адрес, который нет возможности изменить усилиями пользователя без согласия провайдера. Запрос фиксируется на том сервере, к которому подключен компьютер, поэтому любое действие оставляет за собой след на сервере провайдера. Таким образом, использование прокси-серверов создает лишь дополнительную преграду на пути деанонимизации киберпреступника, а маршрут движения запросов можно отследить по физическим IP-адресам, направив запрос к провайдеру.

VPN же в свою очередь создает зашифрованные каналы между точкой отправителя и точкой получателя запроса, создающие зашифрованные в оболочку запросы, суть которых не ясна, если не заниматься их расшифровкой. Такой запрос можно расшифровать при наличии достаточной технической оснащенности. Аналогично зашифрованные запросы идут по прокси-серверам, и в данной ситуации, не расшифровывая запрос прийти к той точке, из которой поступил данный запрос.

Эти средства не имеют безупречной защиты и их нужно использовать осознывая, что найти всю деанонимизировать нас в век информационных технологий будет очень просто. Поэтому часто киберпреступники ищут способы скрыть себя еще больше прибегая к отказу от домашнего интернета и переходят на интернет-кафе, в котором отследить конкретный компьютер, от которого поступил запрос уже не представляется возможным по причине того, что при подключении к бесплатному Wi-fi киберпреступник меняет MAC-адрес своего устройства, что в дальнейшем не позволяет его идентифицировать, но можно установить диапазон нахождения в интернете киберпреступника. И в соответствии с этими данными сотрудники силовых органов будут уже искать не компьютер, а конкретного человека путем опроса сотрудников интернет-кафе, просмотром камер и фиксированием одинаковых людей, тем самым сужая круг поиска.

¹ Усманов Р. А. Установление лиц, использующих сервисы, позволяющие анонимно получать незаконные услуги в интернете (Постановка проблемы).

Все время преступники находят все больше и больше способов скрыть следы преступления, скрыть свою личность, чтобы остаться без наказания и киберпреступники тому не исключение. И каждый способ скрыть преступление имеет либо какие-то недостатки, либо находится противодействие данному способу, о котором не всегда задумываются преступники при попытке избежать наказание.

Список литературы

1. Артамонов В. А., Артамонова Е. В. Методы анонимизации в сети интернет. режим доступа: <http://itzashita.ru/publications/metodyi-anonimizatsii-v-seti-internet.html>.
2. О преступлениях, совершаемых с использованием современных информационно-коммуникационных технологий // Официальный сайт Генеральной прокуратуры Российской Федерации [Электронный ресурс]. Дата обновления: 14.06.2018. Режим доступа: <https://genproc.gov.ru/special/smi/news/news-1431104/>.
3. Рогозин В. Ю. Криминализация Интернета и WEB технологий // Преступность в сфере информационно-телекоммуникационных технологий: проблемы предупреждения, раскрытия и расследования преступлений: сборник материалов всероссийской научно-практической конференции (Воронеж, 22 апреля 2016 г.) / под ред. д-ра юрид. наук. А.Л. Осипенко. Воронеж: Воронежский институт МВД России, 2016. С. 22-26.
4. Симаков А. А., Горев А. И. Защита информационного пространства России от внешних угроз на основе построения Российской государственной анонимной компьютерной сети // Преступность в сфере информационно-телекоммуникационных технологий: проблемы предупреждения, раскрытия и расследования преступлений: сборник материалов всероссийской научно-практической конференции (Воронеж, 22 апреля 2016 г.) / под ред. д-ра юрид. наук. А.Л. Осипенко. Воронеж: Воронежский институт МВД России, 2016. С. 119-124.
5. Состояние преступности в Российской Федерации за январь - декабрь 2017 года // Официальный сайт МВД РФ [Электронный ресурс]. Дата обновления: 19.01.2018. Режим доступа: <https://мвд.рф/reports/item/12167987>.
6. Усманов Р. А. Установление лиц, использующих сервисы, позволяющие анонимно получать незаконные услуги в интернете (Постановка проблемы).
7. Виртуальная Частная Сеть (VPN). Режим доступа: <http://virtualprivatenetworkpptp.blogspot.com/>.

Mikhail S. Pichugov

Student of the Institute of Justice
Ural State Law University
(Russia, Ekaterinburg)
mpicugov843@gmail.com

DEANONYMIZATION OF THE CRIMINAL COMMITTED CRIME ON THE INTERNET

Abstract: The article describes the statistics, examples and methods of committing cyber-attacks, their position in the total mass of crimes at this stage. Describes the tools by which a cybercriminal hides his identity and sweeps away traces, and tools that can be used to uncover the identity of a cybercriminal, or rather, tools for de-anonymizing a hacker who tries to avoid punishment by anonymizing his personality on the Internet

Keywords: cybercrime, cybercriminal, computer, proxy server.

Пучков Владислав Олегович

Магистрант

Уральский государственный юридический университет

(г. Екатеринбург)

puchkov_pravoprocess@mail.ru

ЭЛЕКТРОННЫЕ ДОКАЗАТЕЛЬСТВА В ГРАЖДАНСКОМ ПРОЦЕССУАЛЬНОМ ПРАВЕ США*

Аннотация: В статье рассматриваются особенности электронных доказательств в гражданском процессе США. На основе анализа законодательства, правовой доктрины и судебной практики автор обосновывает характер электронных доказательств как правового явления *sui generis*. Исследуются особенности использования электронных доказательств в судебном доказывании («стандарт достоверности», «правило наилучшего доказательства»). Доказывается оправданность различий в судебной оценке различных видов электронных доказательств.

Ключевые слова: гражданский процесс, доказательства, электронные доказательства, стандарт достоверности, правило наилучшего доказательства.

Развитие информационных технологий, их внедрение во все сферы жизни общества оказывает существенное влияние на актуальное состояние социально-экономических процессов. С этой позиции информатизация социальной деятельности, опосредующая особую динамику общественных отношений, нуждается в теоретической концептуализации не только с технической, технологической позиции, но и с точки зрения права как фундаментального социально-нормативного регулятора. В заданном контексте наиболее ярко правовые аспекты использования информационных технологий проявляют себя именно тогда, когда они вовлекаются в орбиту юридической деятельности, и в первую очередь – в систему процессуально-правовых отношений. Будучи включенными в данную систему, явления информационно-технологического порядка приобретают особые правовые свойства, обусловленные не только их характеристиками *per se*, но и спецификой процессуальной деятельности. К числу таких явлений относятся в первую очередь электронные доказательства. Следует подчеркнуть, что, как отмечают исследователи, наибольшее распространение электронные доказательства (*digital evidence*) получили в США, где уже с конца 1980-х – начала 1990-х годов начала формироваться практика их применения в гражданском судопроизводстве¹. В этой связи обращение к опыту США в сфере использования электронных доказательств представляет интерес как с теоретической, так и с прикладной точки зрения.

Впервые понятие электронного доказательства в США было сформулировано в решении Апелляционного суда 9-го округа по делу *U.S. v. Bonallo*² в 1988 г. Как отмечается в данном судебном акте, электронное доказательство представляет собой «данные, полученные посредством применения компьютерной техники, и в отношении

* Исследование выполнено при финансовой поддержке Российского фонда фундаментальных исследований в рамках научного проекта 18-29-16148 «Исследование в части формирования единой цифровой среды доверия, ее элементов и принципов работы. Определение механизмов защиты информации, использующихся при формировании единой цифровой среды доверия. Исследование механизмов контроля целостности при формировании распределенных реестров. Выработка предложений по актуализации нормативно-правовой базы Российской Федерации в части регулирования обеспечения информационной безопасности и защиты информации, в частности документов ограниченного распространения».

¹ Manes G. W., Downing E., Watson L., Thrutchley Ch. New Federal Rules and Digital Evidence // Annual ADFSL Conference on Digital Forensics, Security and Law. 2007, Vol. 3. Arlington: ADFSL Press, 2007. P. 32 – 33.

² U.S. v. Bonallo (1988), 858 F.2d 1427.

которых можно достоверно установить, от какого конкретно эти данные исходят». Тем самым более 30 лет назад в США было установлено особое правило использования электронных доказательств – так называемый «стандарт достоверности» (*standard of authenticity*). Согласно этому правилу, если доказательство выполнено в электронной форме (например, представляет собой электронное сообщение или электронный документ), то оно может быть использовано только в том случае, если будет установлен источник их происхождения, а также эквивалентность их содержания с содержанием какого-либо материального носителя. Впоследствии эта позиция нашла свое отражение в статье 901 Федеральных правил о доказательствах¹ (*Federal Rules of Evidence*). Как подчеркнул Апелляционный суд штата Калифорния в решении по делу *Aguimatang v. California State Lottery*², «стандарт достоверности» применительно к электронным доказательствам представляет собой частный случай так называемого «правила наилучшего доказательства» (*best evidence rule*), согласно которому копия любого письменного документа должна быть содержательно подтверждена оригиналом (статья 702 Федеральных правил о доказательствах). Тем самым в заданном контексте электронные доказательства были определены в качестве особого вида письменных доказательств, поскольку именно к ним применяется «правило наилучшего доказательства»³. В целом общепринятым в праве США признается подход, выраженный Апелляционным судом штата Висконсин в постановлении по делу *State v. Schroeder*⁴. В соответствии с данным подходом сторона, представляющая электронный документ, сообщение либо иную информацию в электронной форме должна любым не противоречащим законом способом подтвердить ее достоверность. С этой целью, как неоднократно подчеркивал Верховный Суд США (см., например, решение по делу *Dye v. U.S.*⁵) могут быть использованы любые возможные методы: заверение независимым специалистом, предоставление ксерокопии электронных материалов, а также проведение осмотра такого доказательства по месту его нахождения⁶.

В целом следует отметить, что в США правовой режим электронных доказательств является однозначно определенным: такие доказательства понимаются как особая форма письменных доказательств, а, следовательно, особенности письменных доказательств в гражданском процессе обуславливают соответствующие особенности электронных доказательств. При этом «стандарт достоверности», применяемый к оценке достоверности электронных доказательств, имеет более широкое содержание по сравнению с «правилом наилучшего доказательства», поскольку предполагает не только соотнесение содержания электронного материала с его ксерокопией, но и вариативный спектр подтверждения содержательной достоверности электронных доказательств.

Список литературы

1. Cole K. A., Gupta S., Gurugubelli D., Rogers M. K. A Review of Recent Case Law Related to Digital Forensics: The Current Issues // Annual ADFSL Conference on Digital Forensics, Security and Law. 2007, Vol. 2. Arlington: ADFSL Press, 2015.

¹ Federal Rules of Evidence // U.S.C. Title 28.

² *Aguimatang v. California State Lottery* (1991), No. C007401. Third Dist. Sep 25, 1991.

³ Решетникова И.В. Доказательственное право Англии и США. 2-е изд., перераб. и доп. М.: Городец, 1999. С. 150 – 152.

⁴ *Schroeder v. Schroeder* (1981), 100 Wis. 2d 625.

⁵ *Dye v. U.S.* (1997), 121 F.3d 1399.

⁶ Cole K. A., Gupta S., Gurugubelli D., Rogers M. K. A Review of Recent Case Law Related to Digital Forensics: The Current Issues // Annual ADFSL Conference on Digital Forensics, Security and Law. 2007, Vol. 2. – Arlington: ADFSL Press, 2015. P. 95 – 97.

2. Manes G. W., Downing E., Watson L., Thrutchley Ch. New Federal Rules and Digital Evidence // Annual ADFSL Conference on Digital Forensics, Security and Law. 2007, Vol. 3. Arlington: ADFSL Press, 2007.

3. Решетникова И. В. Доказательственное право Англии и США. 2-е изд., перераб. и доп. М.: Городец, 1999.

Vladislav O. Puchkov

Master Student

Ural State Law University

(Russia, Yekaterinburg)

puchkov_pravoprocess@mail.ru

DIGITAL EVIDENCES IN U.S. CIVIL PROCEDURE

Abstract: The article deals with the specifics of digital evidence in U.S. civil procedure. Basing on the analysis of legislation, legal doctrine and practice author proves the *sui generis* character of digital evidences. The author researches the specificity of the usage of such evidences in judicial proving (e.g. standard of authenticity, best evidence rule). Author justifies the idea of different approach by courts in evaluation of different types of digital evidences.

Доказывается оправданность различий в судебной оценке различных видов электронных доказательств.

Keywords: civil procedure, evidence, digital evidence, standard of authenticity, best evidence rule.

Пушкарева Александра Игоревна

Студент Институт Юстиции
Уральский государственный юридический университет
(г. Екатеринбург)
pushkareva.alexandra@inbox.ru

Сытикова Регина Игоревна

Студент Институт Юстиции
Уральский государственный юридический университет
(г. Екатеринбург)

ВОЗМОЖНОСТИ ИСПОЛЬЗОВАНИЯ УСЛУГ СУРРОГАТНОГО МАТЕРИНСТВА ДЛЯ ПАР, ПРИНАДЛЕЖАЩИХ К ЛГБТ-СООБЩЕСТВУ

Аннотация: В данной статье анализируются правовые аспекты суррогатного материнства среди разных социальных групп, а также среди вызывающего интерес ЛГБТ-сообщества. Мы выясним, возможно ли осуществить данную процедуру на примере конкретных стран: России, Франции, США. Подробно рассмотрены как положительные, так и отрицательные стороны данного явления и подведены итоги в соответствии с изученными материалами и статистическими данными с опорой на англосаксонское и континентальное право.

Ключевые слова: суррогатное материнство, ЛГБТ-сообщество, правовые семьи, право.

Матери-одиночки, суррогатные матери, однополые родители... Репродуктивные технологии перевернули наши представления о родственных отношениях. Подарив счастье стать родителями тысячам людей, но и породив множество вопросов: у всех ли есть право на потомство или желание иметь ребенка не всегда «законно»?

Суррогатное материнство представляет собой вынашивание и рождение ребенка (в том числе преждевременные роды) по договору, заключаемому между суррогатной матерью (женщиной, вынашивающей плод после переноса донорского эмбриона) и потенциальными родителями, чьи половые клетки использовались для оплодотворения, либо одинокой женщиной, для которых вынашивание и рождение ребенка невозможно по медицинским показаниям¹ [1].

Суррогатное материнство как таковое появилось в конце прошлого столетия, а именно в 1976 году в Соединенных Штатах Америки. Появление обусловлено великими достижениями науки того времени в области вспомогательных репродуктивных технологий.

Так, в п. 2 Постановлении Специального экспертного комитета Совета Европы по биологической этике и искусственным методам деторождения (Принцип 15, 1989) указано: «Ни один контракт или соглашение между суррогатной матерью и тем лицом или парой, для которых она вынашивает ребенка, не должны иметь законной силы».

Воспитание детей однополыми парами, а также возможность разрешения таким парам усыновления детей или получения ими права пользоваться услугами суррогатного материнства является предметом научных и общественных дискуссий. Самый популярный у гомосексуальных женщин способ, когда одна из партнерш выступает

¹ Об основах охраны здоровья граждан в Российской Федерации: Федеральный закон от 21.11.2011 N 323-ФЗ (ред. от 06.03.2019) // СПС КонсультантПлюс [Электронный ресурс]. Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_121895/ (дата обращения: 18.05.19).

донором яйцеклетки, а вторая – суррогатной матерью. В прежней семье из нескольких поколений были мама и папа – и множество взрослых родственников. И они, кстати, своим влиянием могли компенсировать то, что не получалось у родителей. Сейчас семьи стали очень узкими, возможностей компенсации меньше. Но с другой стороны, таким влиянием, такой компенсацией, возможно, способно стать то, что и родителей тоже может быть больше, чем два.

В России данной процедурой могут воспользоваться только лица мужского и женского пола, как состоящие, так и не состоящие в браке, а также одинокие женщины.

Что касается Франции, то данная процедура запрещена законом¹. Но ЕСПЧ разрешил французским гражданам пользоваться услугами суррогатного материнства за пределами страны и наложил соответствующие санкции на государство. Франция стала восьмой страной в Европе и четырнадцатой в мире, где узаконены однополые браки²[3].

Вызывает большой диссонанс отношение России к ЛГБТ-сообществу: ущемлению их прав, нарушению свободы выбора. В законодательстве не предусмотрены однополые браки, не говоря уже о предоставлении услуг суррогатного материнства таким парам. Русская православная церковь, позиция которой приобретает всё больший вес, и вовсе против любых помогающих технологий, полагая, что человек выходит за рамки дозволенного ему свыше и пытается присвоить себе божественные функции. «Нельзя идти против Божественного закона. Потому что только Божественный закон является абсолютным. В нём – полнота мудрости и милости», – высказался патриарх Кирилл в Сретенском монастыре Москвы³.

Обратимся к англосаксонской правовой семье, в частности, рассмотрим нормы права США, касающиеся вышеупомянутого вопроса. В таких штатах, как Флорида и Калифорния действует демократичное законодательство в этой сфере (Калифорнию даже считают мировым центром в этой области (в том числе и по научным достижениям)). Так, за помощью могут обратиться одинокие мужчины и однополые партнеры. Но в Мичигане и Вирджинии, например, действует полный запрет на использование услуг суррогатного материнства.

Суррогатная мама – единственный на сегодняшний день альтернативный репродуктивный метод для ЛГБТ-пар. Известный всему миру певец и композитор Элтон Джон в январе 2013 года стал отцом второй раз. Оба его сына рождены одной и той же суррогатной матерью, имя которой держится в строжайшем секрете. Несмотря на существующие протесты против меньшинств, американское агентство альтернативной репродукции утверждает, что «нетрадиционных родителей» в США уже больше миллиона⁴.

Суррогатное материнство среди ЛГБТ-пар поддерживается большим количеством стран, поскольку люди видят в этом следующие преимущества:

1. Представители вышеназванного сообщества ввиду отсутствия возможности естественного оплодотворения прибегают к суррогатному материнству, тем самым улучшают демографические показатели государства, в котором они проживают.

2. При использовании ЛГБТ-парами данной услуги повышается приток денежных средств в казну государства (налоги с процедуры), что способствует увеличению капитала.

¹ Суррогатное материнство во Франции [Электронный ресурс]. Режим доступа: <https://суррогатные-матери.рф/surrogatnoye-materinstvo-2019/24-strani/strani/850-surrogatnoe-materinstvo-vo-frantsii.html> (дата обращения: 10.05.19).

² Дронова Ю. А. Как регулируется суррогатное материнство в зарубежном законодательстве // Что нужно знать о суррогатном материнстве / Ю. А. Дронова. Режим доступа: <https://lawbook.online/semeynoe-pravo-rossii-kniga/kak-reguliruetsya-surrogatnoe-materinstvo-43895.html> (дата обращения: 10.05.19).

³ Почему в России не любят ЛГБТ? Какие права есть у меньшинств, как к ним относятся? [Электронный ресурс]. Режим доступа: <https://znay.co/130-pochemu-v-rossii-ne-lyubyat-lgbt.html> (дата обращения: 10.05.19).

⁴ Права ЛГБТ в США // Википедия – свободная энциклопедия [Электронный ресурс]. Режим доступа: https://ru.wikipedia.org/wiki/Права_ЛГБТ_в_США (дата обращения: 10.05.19).

3. Это единственный возможный способ появления на свет биологического ребенка в однополых семьях нежели усыновление/удочерение.

4. Однополые родители не подвержены дискриминации по гендерному типу, что нередко случается в гетеросексуальных парах, в связи с этим дети ЛГБТ-пар переживают меньшее количество стрессовых ситуаций.

Но не стоит забывать о негативной стороне данного аспекта:

1. Суррогатное материнство среди ЛГБТ-пар способствует вытеснению традиционного типа семьи, закрепившегося во всех странах мира, в частности и в Российской Федерации.

2. Дети, воспитывающиеся в однополых семьях, могут подвергаться критике со стороны окружающих, что негативно влияет на их психоэмоциональное состояние.

3. Это противоречит морали. С религиозной точки зрения суррогатное материнство не самый страшный, но порицаемый грех.

4. Однополые браки нарушают нормальную специализацию полов: ребенок может затрудняться в выборе собственной половой принадлежности.

Подводя итоги, мы пришли к выводу, что право рассмотренных нами стран по-разному регулирует вопрос суррогатного материнства, а также ЛГБТ-сообщества. А именно в Российском законодательстве не регулируется вопрос ЛГБТ-браков. Но распространено суррогатное материнство среди традиционных семей. Что касается Франции, то суррогатное материнство там запрещено под страхом юридической ответственности в отличие от законодательства США, где данная услуга свободно распространена среди однополых браков.

По нашему мнению, суррогатное материнство среди ЛГБТ-пар недопустимо, поскольку это может оставить неизгладимый отпечаток на детской психике. У ребенка может нарушиться идентичность и самоопределение половой позиции. Но это личный выбор каждого, субъективное мнение, и поэтому мы должны уважать взгляды и ценности друг друга.

Список литературы

1. Дронова Ю. А. Как регулируется суррогатное материнство в зарубежном законодательстве // Что нужно знать о суррогатном материнстве / Ю. А. Дронова. Режим доступа: <https://lawbook.online/semeynoe-pravo-rossii-kniga/kak-reguliruyetsya-surrogatnoe-materinstvo-43895.html>

2. Почему в России не любят ЛГБТ? Какие права есть у меньшинств, как к ним относятся? [Электронный ресурс]. Режим доступа: <https://znay.co/130-pochemu-v-rossii-ne-lyubyat-lgbt.html>.

3. Права ЛГБТ в США // Википедия – свободная энциклопедия [Электронный ресурс]. Режим доступа: https://ru.wikipedia.org/wiki/Права_ЛГБТ_в_США.

4. Суррогатное материнство во Франции [Электронный ресурс]. Режим доступа: <https://суррогатные-матери.рф/surrogatnoye-materinstvo-2019/24-strani/strani/850-surrogatnoe-materinstvo-vo-frantsii.html>.

Alexandra I. Pushkareva

Student of Institute of Justice

Ural State Law University

(Russia, Yekaterinburg)

pushkareva.alexandra@inbox.ru

Regina I. Sytikova

Student of Institute of Justice

Ural State Law University

(Russia, Yekaterinburg)
sytkova2000@mail.ru

THE ABILITY TO USE SURROGATE MOTHERHOOD FOR COUPLES WHO BELONG TO THE LGBT COMMUNITY

Annotation: Article analyzes the legal aspects of surrogacy among different social groups, as well as among, arousing interest, the LGBT community. We will find out whether it is possible to carry out this procedure on the example of specific countries: Russia, France and USA. Let us consider in detail both positive and negative aspects of this phenomenon and summarize in accordance with the materials and statistics studied, based on Anglo-Saxon and continental law.

Keywords: surrogacy, LGBT community, legal families, law.

Рачева Нелли Витальевна

Кандидат юридических наук, доцент, доцент кафедры криминалистики
Уральский государственный юридический университет
Екатеринбург
ekaterinburg@mail.ru

Скорб Яна Владимировна

Студент Института государственного и международного права
Уральский государственный юридический университет
Россия, Екатеринбург
iana.skorb@gmail.com

**СОВРЕМЕННЫЕ ТЕХНОЛОГИИ СОБИРАНИЯ И ИССЛЕДОВАНИЯ
ЭЛЕКТРОННО-ЦИФРОВЫХ ДОКАЗАТЕЛЬСТВ ПРИ РАССЛЕДОВАНИИ
ПРЕСТУПЛЕНИЙ, СВЯЗАННЫХ С НЕЗАКОННЫМ СБЫТОМ
НАРКОТИЧЕСКИХ СРЕДСТВ, ПСИХОТРОПНЫХ ВЕЩЕСТВ И ИХ АНАЛОГОВ**

Аннотация: в статье рассмотрены основные виды электронной-цифровых доказательств, используемых при расследовании преступлений, связанных с незаконным сбытом наркотических средств, психотропных веществ и их аналогов. Сформулировано понятие электронно-цифровых доказательств и приведен перечень объектов, которые могут быть к ним отнесены. Указаны особенности собирания электронных доказательств, имеющих значение для уголовного дела, связанного с незаконным распространением наркотических средств. Также в статье приведены некоторые новейшие приемы и способы проведения компьютерно-технических экспертиз.

Ключевые слова: электронно-цифровые доказательства, собирание доказательств, допустимость доказательств, компьютерно-техническая экспертиза, электронные носители информации, наркотические средства.

Глобализация и информатизация общества двадцать первого столетия привели к созданию единого мирового пространства - информационного пространства, которое образует сеть Интернет и другие телекоммуникационные сети, которые позволяют устанавливать анонимное соединение и облегчают возможность совершения противоправного деяния. Например, в преступном сообществе широко известны скрытые сети DarkNet, Tor.

Основной проблемой для уголовного судопроизводства в Российской Федерации стало разнообразие новых способов совершения отдельных видов преступлений. В последние годы особое внимание правоохранительных органов приковано к проблеме стремительного распространения в России в больших объемах новых форм синтетических наркотических средств и психотропных веществ, которые в преступном обиходе называют: «смайлики», «соли для ванн», «метель», «чёрная мамба». Согласно официальной статистике МВД России за 2018 год в Российской Федерации выявлено 151,3 тысяч преступлений, связанных с незаконным оборотом наркотических средств, что на 4,6% меньше, чем за аналогичный период прошлого года. Однако эти данные не позволяют сделать вывод о том, что число данных преступлений сократилось. Официальная статистика говорит лишь о том, что преступления, связанные с незаконным оборотом наркотических средств, психотропных веществ и их аналогов, стало труднее выявлять. Нужно отметить, что по состоянию преступности в Российской Федерации, за январь-сентябрь 2018 года число выявленных преступлений, совершённых с целью сбыта

наркотических средств, психотропных веществ или их аналогов по сравнению с январем - сентябрем 2017 года увеличилось на 3,6 %¹.

Незаконный сбыт наркотических средств и иных психотропных веществ в России с каждым годом все больше видоизменяется, приобретает новые формы, адаптируясь к современным реалиям. Соответственно, правоохранительные и законодательные органы нуждаются в разработке новых технологий расследования преступлений, связанных с незаконным распространением наркотических средств, психотропных веществ и их аналогов.

В последние годы появились новые способы совершения преступлений в сфере незаконного оборота наркотических средств, связанные с их распространением через сеть Интернет. Для распространения наркотических средств, психотропных веществ и их аналогов в информационной теневой сети DarkNet созданы специальные сайты, например, Hydra2wed.com, а также используются такие мессенджеры, как WhatsApp, Viber, Facebook Messenger, Telegram. Кроме этого, преступники создают свои собственные анонимные сети, что помогает им латентно и безнаказанно совершать преступления, цели которых раньше достигались традиционными путями.

Говоря о субъектах преступлений данной категории нужно отметить, что основную роль в составе преступной группы играет не только сбытчик наркотических средств, но и организаторы, изготовители, переработчики, перевозчики, «закладчики», «трафаретчики» и «бегунки». Коммуникация между ними происходит бесконтактно, путем переписки в анонимных сетях и мессенджерах. Оплата за товар производится теперь также бесконтактным путем. Это существенно отличается от того, что было в недалеком прошлом - в 90-х годах прошлого столетия, когда для сбыта наркотических средств преступники искали «закладчиков» на улице или среди родственников и знакомых (чаще всего в этой роли выступали подростки). Оплата за наркотические средства производилась наличными денежными средствами.

Сейчас в социальных сетях есть целые банки «объявлений о работе», где размещаются требования к «закладчикам» и «курьерам», условия работы и обязанности. Сама сущность сети Интернет благоприятна для совершения преступлений, так как она обладает такими свойствами как трансграничность, глобальность, анонимность, имеет широкий охват аудитории, что создает преступникам преимущества на всех этапах совершения преступлений. Соккрытие преступлений может реализовываться путем уничтожения виртуальных следов деятельности, то есть удалением данных с персонального компьютера или телефона непосредственно после совершения преступления.

Совершение преступлений такими способами значительно затрудняет процесс доказательства причастности определенных лиц к противоправному деянию. Поэтому, в ходе расследования незаконного сбыта наркотических средств, психотропных веществ и их аналогов, необходимы тщательная подготовка и эффективное производство следственных действий, связанных с собиранием электронно-цифровых доказательств бесконтактного общения и использования Интернета, как средства совершения преступления.

Процесс информатизации общества не стоит на месте и в связи с этим, с каждым годом использование письменных документов, как в целом и всего бумажного документооборота, становится нецелесообразным. На смену им приходят электронные документы, а также видео- или аудиозаписи в цифровом формате. В Российской Федерации в силу чрезмерно быстрого перехода страны от эпохи индустриального развития к информационному произошла подмена терминов «электронный» и

¹ Краткая характеристика состояния преступности в Российской Федерации за январь - сентябрь 2018 года // Официальный сайт МВД РФ [Электронный ресурс]. Режим доступа: <https://мвд.рф/reports/item/14696015> (дата обращения: 18.05.2019).

«цифровой», в нашем языке эти понятия превратились в взаимозаменяемые. Однако это не так и нужно первоначально обратиться к толкованию данных терминов. «Электронный» - данный термин предназначен для того, чтобы охватить любое или все устройства, или системы, действующие на основе электричества. В число электрических, электронных, программируемых электронных устройств входят:

- электромеханические устройства (электрические);
- полупроводниковые непрограммируемые электронные устройства (электроника);
- электронные устройства, основанные на компьютерных технологиях (программируемые электронные устройства)¹.

«Цифровой» – термин, описывающий информацию, выраженную при помощи чисел. Такие данные как слова, изображения, звуки, представляются в виде набора цифр (1 и 0) в двоичной системе, которая используется в компьютерах, так, например, на компакт-дисках информация хранится в цифровом виде, нули и единицы изображаются при помощи углублений на его поверхности.

Но прежде чем называть те или иные объекты электронно-цифровыми доказательствами, нужно разобраться, что же все-таки к ним относится. В настоящее время действующим законодательством не определено понятие электронно-цифрового доказательства. Для того, чтобы сформулировать понятие «электронно-цифровые доказательства», обратимся к Федеральному закону «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ. Согласно статье 2 данного Федерального закона сведения могут быть представлены в виде электронного документа, сообщения, сайта в глобальной сети Интернет или страницы этого сайта. Исходя из этого, можно сделать вывод, что круг электронных носителей, которые могут выступать электронно-цифровыми доказательствами, достаточно конкретный. Данные объекты могут быть отнесены к закрепленным в УПК РФ доказательствам, как вещественные доказательства и иные документы. Но необходимо иметь ввиду, что данные объекты информации для использования в качестве доказательств в уголовном деле, должны соответствовать хотя бы одному из условий, перечисленных в ч. 1 ст. 81 УПК РФ, а именно:

- 1) служили орудиями, оборудованием или иными средствами совершения преступления или сохранили на себе следы преступления;
- 2) являются предметом преступления;
- 3) представляют имущество (деньги, ценные бумаги), полученное в результате совершения преступления или нажитое преступным путем;
- 4) служат средством для обнаружения преступления и установления обстоятельств по уголовному делу.

Электронно-цифровые доказательства являются разновидностью доказательств в целом, при этом они обладают особенностями: содержатся на особых носителях (жестких дисках, серверах, сайтах в сети Интернет, флэш-картах, СИМ-картах и др.) и для их прочтения необходимы специальные технические устройства. На основании выделенных особенностей можно определить «электронно-цифровые доказательства» как сведения о фактах, имеющих значение для установления обстоятельств, которые подлежат доказыванию по уголовному делу, закрепленные в форме цифровой информации, прочтение которой невозможно без использования специальных технических устройств.

Электронно-цифровые доказательства должны обладать свойствами относимости, допустимости и достаточности, что обеспечивает их законность. Говоря о критерии

¹ п. 3.2.13 ГОСТ Р МЭК 61508-4-2012 Функциональная безопасность систем электрических, электронных, программируемых электронных связанных с безопасностью. Часть 4. Термины и определения. М.: Стандартинформ, 2014.

допустимости, нужно сказать, что доказательства в цифровой форме должны соответствовать общим критериям, которые присущи всем доказательствам: обязательное составление протокола, собирание доказательств специально уполномоченным лицом, указанным в законе, участие понятых и т.д. Также требуется их соответствие специальным критериям, которые присущи только электронно-цифровым доказательствам. Так, например, компьютерная экспертиза должна проводиться исключительно компетентным специалистом в сфере компьютерных и иных современных технологий; осмотр сайта в сети Интернет должен также проводиться с участием специалиста и понятых и др. Иными словами, доказательства данного вида должны подвергаться более строгой оценке, для чего необходимо использовать специальные устройства, а также привлекать лиц, обладающих познаниями в сфере современных технологий.

Известно, что электронно-цифровые доказательства могут быть подвергнуты изменению, а также уничтожены без особого труда. Исходя из этого отдельное внимание нужно уделить особенностям собирания электронно-цифровых доказательств. К ним относятся: оперативность производства необходимых действий, участие при проведении следственных действий специалиста в области компьютерных и иных современных технологий, а также наличие устройств, обеспечивающих собирание данных доказательств: ими могут выступать персональный компьютер или мобильное устройство.

Для собирания электронно-цифровых доказательств при расследовании преступлений, связанных с незаконным сбытом наркотических средств, психотропных веществ и их аналогов, помимо типовых следственных действий, следует особо выделить обыск, выемку и осмотр. В настоящее время следователь не может проводить осмотр электронных и цифровых устройств в качестве самостоятельного следственного действия, так как отсутствует достаточная законодательная регламентация. В связи с чем, осмотр устройств, связанный с извлечением информации, происходит с помощью такого следственного действия, как осмотр предметов. Данное следственное действие происходит с участием специалиста, поскольку навыками работы с электронными устройствами обладает именно он. В протоколе осмотра предмета (электронного устройства) следователь описывает все действия, осуществляемые специалистом, а также фиксирует информацию, полученную в ходе следственного действия. Осмотр предмета, как следственного действия связан с собиранием доказательств путем внешней проверки его конструкции, выявлении индивидуальных черт, отличительных признаков от идентичных предметов и т. д. Для проведения данного следственного действия нужно предусмотреть, что информация, содержащаяся на электронном носителе, носит сугубо личностный характер. Но не каждая информация имеет содержательное наполнение и, в связи с этим, различают данные, которые можно получить из мобильного устройства без решения суда и с его разрешения. К первой категории относятся: входящие, исходящие звонки, заметки в календаре, записная книжка, напоминания в календаре и т. п. Ко второй категории относится информация из СМС-сообщений, сообщения из электронной почты, переписки в социальных сетях, чатах, фото, находящиеся в памяти электронных устройств, в этом случае необходимо обращаться в суд с ходатайством на проведения осмотра электронного устройства.

Для доказывания бесконтактного способа совершения преступления сначала необходимо проанализировать информацию о взаимодействии электронных устройств сбытчика, посредника и покупателя наркотиков. Получить данную информацию следователь может путем запроса у оператора связи либо непосредственно из самого электронного устройства, изъятого у лица в ходе обыска (выемки). Затем следователь может получить информацию от банков о финансовых операциях сбытчика и покупателей наркотических веществ. При этом, электронно-цифровыми доказательствами выступает информация об Интернет-общении сбытчика со своими клиентами, проводимом с помощью персонального компьютера, телефона, смартфона, планшета и иных новых

технических устройств, с помощью которых возникает возможность бесконтактного, анонимного общения.

Для изъятия электронно-цифровых доказательств уголовно-процессуальным законом статьей 164.1 УПК РФ предусмотрена возможность копирования информации с электронных носителей на другие электронные носители информации. При этом необходимо использовать переносные цифровые устройства. Ими могут выступать: компьютер, ноутбук, планшет, мобильный телефон, накопитель USB-флеш или CD-диск. Основанием для запрета копирования информации с электронного носителя может являться заявление специалиста, связанного с тем, что это действие может привести к утрате криминалистически значимой информации или её искажению. В остальных случаях возможно осуществление копирования информации на другие электронные носители по ходатайству законного владельца. Все действия, производимые с электронными носителями и информацией на электронном устройстве, должны быть зафиксированы в протоколе следственного действия.

Однако нередко возникают ситуации, когда информация содержится не на материальных носителях, а хранится на странице интернет сайта или в базе данных. При работе с такими доказательствами сначала проводят их осмотр, затем рекомендуется зафиксировать и произвести изъятие всех обнаруженных средств электронной техники, с последующим изучением имеющейся на ней информации. Изъятие средств компьютерной техники ускоряет процесс проведения следственного действия, дает возможность направить все силы на поиск иных материальных следов, имеющих отношение к делу (наркотические средства, содержащиеся в виде таблеток, порошка, фармацевтических препаратов в ампулах, средства производства и фасовки наркотических средств, документы и т. д.). К достоинствам такого способа изъятия электронно-цифровых доказательств относится возможность в последующем, привлекая необходимых специалистов, изучить всю информацию, содержащуюся в памяти компьютера. Также, во время проведения самого следственного действия не требуется присутствие специалиста.

Так, Советским районным судом г. Орск г. Я. был признан виновным в совершении преступления, предусмотренного ч. 3 ст. 30, п. «г» ч. 4 ст. 228.1 УК РФ – покушение на сбыт наркотических средств в крупном размере. В апелляционной жалобе осужденный просил отменить приговор, среди прочего ссылаясь на то, что изъятие у него мобильного телефона, являющегося электронным носителем информации, было произведено сотрудниками Линейного отдела МВД России на транспорте без участия специалиста в нарушение ч. 3.1. ст. 183 УПК РФ.

Суд апелляционной инстанции признал указанный довод гр. Я. необоснованным, указав, что из смысла ч. 3.1. ст. 183 УПК РФ участие специалиста при производстве выемки в ходе изъятия электронных носителей информации требуется при наличии нуждаемости в данном специалисте, то есть когда необходимо применить специальные познания и навыки. В частности, если при производстве выемки производится копирование информации на другие электронные носители информации, участие специалиста обязательно, так как это связано с риском утраты или изменения информации. При этом, из материалов дела следует, что при выемке следователь пользовался обычными функциями просмотра телефона, не прибегая к необходимости поиска и открытия закрытых для общего доступа файлов, что говорит о законности произведенных действий¹.

Кроме копирования и изъятия электронной информации, представляется возможным в момент проведения следственного действия сделать скриншоты страниц интернет сайтов с информацией, имеющей значение по уголовному делу. Затем производится распечатка скриншотов интернет – страницы. Здесь важно отметить, что

¹ Апелляционное определение Судебной коллегии по уголовным делам Оренбургского областного суда от 03.11.2016 г. по делу № 22-4229/2016

имеется техническая возможность изменить содержание скриншотов распечатываемой информации. В связи с этим, основной гарантией достоверности распечатываемой информации, содержащейся на странице сайта в сети Интернет, является наличие понятий, которые должны подтвердить идентичность текста информации. После соответствующего оформления, протокол следственного действия подписывается всеми участниками и к нему прилагаются диск с записью скриншота экрана электронного устройства, фототаблица со снимком экрана и распечатанные материалы с сайта сети Интернет.

Для исследования изъятой криминалистически значимой информации в электронном виде, производится судебная компьютерно-техническая экспертиза (СКТЭ), которая представляет собой самостоятельный род судебных экспертиз и относится к классу инженерно-технических. Компьютерно-техническая экспертиза проводится в целях: определения статуса объекта как компьютерного средства или иного технического устройства, выявления и исследования его использования в расследуемом преступлении, а также для получения доступа к информации на электронных носителях с последующим всесторонним ее изучением.

Для более полного охвата технологических особенностей и свойств объектов, предъявляемых для экспертизы, выделяются следующие виды компьютерно-технических экспертиз: аппаратно-компьютерная, программно-компьютерная, информационно-компьютерная, компьютерно-сетевая экспертизы. Основными видами СКТЭ при расследовании преступлений, связанных с оборотом наркотических средств, выступают информационно-компьютерная экспертиза (данных), которая позволяет завершить целостное построение доказательственной базы, так как ее целью является поиск, обнаружение, оценка, анализ и информации, созданной преступником в компьютерной системе и судебная компьютерно-сетевая экспертиза

Объектами экспертизы могут выступать различные компьютерные системы (персональные компьютеры, ноутбуки, планшетные компьютеры и др.), разнообразные электронные накопители данных: от жестких-дисков, CD-ROM, DVD, магнитных накопителей до RAID – массивов (дисковый массив, т.е. комплекс из нескольких устройств, - жестких дисков).

Важным при проведении СКТЭ является соблюдение принципов сохранности цифровых данных, которые сегодня приведены в Инструкции по обращению с цифровыми изображениями и аудио- доказательствами¹ и Практическом руководстве по исследованию цифровых доказательств². В настоящее время Международной организацией по компьютерным доказательствам (IOCE) приняты шесть принципов, которыми надлежит руководствоваться при поиске, обнаружении, фиксации, изъятии, исследовании и хранении цифровых доказательств:

1. При работе с цифровым доказательством должны быть соблюдены все общие судебно-экспертные и процессуальные положения;
2. При изъятии цифровых доказательств производимые действия не должны изменять цифровое доказательство;
3. Если лицу необходимо получить доступ к оригинальному цифровому доказательству, лицо должно иметь соответствующую подготовку;
4. Вся деятельность по изъятию, доступу, хранению или передаче цифровых доказательств должна быть полностью задокументирована, защищена и доступна для анализа;
5. Вся деятельность по изъятию, доступу, хранению или передаче цифровых доказательств должна быть полностью задокументирована, защищена и доступна для анализа;

¹ Инструкция по обращению с цифровыми изображениями и аудиодоказательствами, IOCE, Декабрь, 2000 г.

² Практическое руководство по исследованию цифровых доказательств, IOCE, Май 2002 г.

6. Любая организация, которая отвечает за изъятие, доступ, хранение или передачу цифровых доказательств отвечает за соответствие данным принципам. Соблюдение указанных выше принципов обязательно при проведении любых судебных компьютерно-технических экспертиз, связанных с исследованием электронных и цифровых носителей информации.

При производстве СКТЭ успешно применяются следующие приемы: взлом парольных защит, моделирование памяти электронных объектов в памяти технического устройства, в памяти компьютера, с помощью программного инструментария Cardreader CardLabs, Zert и другие, что позволяет получить значимую информацию для расследования незаконного сбыта наркотических средств, психотропных веществ и их аналогов.

Проведение компьютерно-технических экспертиз предусматривает мероприятия по обеспечению сохранности цифровой информации. Среди данных мероприятий выделяются следующие: при подключении носителя цифровой информации к тестовому компьютеру эксперта используются аппаратные средства блокирования уничтожения или сохранения информации, после чего производится полное копирование цифровой информации на специально выделенные экспертом зоны на тестовом компьютере (так называемое создание «образа» исследуемого носителя цифровой информации). Именно над «образом» эксперт и осуществляет исследование. Данные действия должны проводиться только с использованием специализированного программного обеспечения, использование которого должно быть указано в экспертном заключении.

На подготовительном этапе проведения экспертизы выполняются следующие действия:

- 1) Проверка физического размера диска и сравнение его с размером всех областей дискового пространства;
- 2) Определение и сравнение размеров логических разделов с размером диска для определения информации об удаленных разделах или о неиспользуемом дисковом пространстве;
- 3) Получение информации о настройках временных зон для каждого;
- 4) Переименование разделов накопителя на жёстких магнитных дисках так, как это необходимо («С», «D» и т.д.);
- 5) Сбор системной информации:
 - определение типа ОС, даты установки ОС; перечня установленных и запускаемых приложений; имени пользователя и имени компьютера, и т.п.;
 - получение информации о профиле пользователя (имя, SID, дата создания и последнего входа в систему);
- 6) Экспресс-анализ данных:
 - анализ сигнатуры файлов, просмотр переименованных файлов;
 - определение зашифрованных файлов
 - определение и монтирование файлов-образов, контейнеров, архивов – ZIP, RAR, E-mail-контейнеры и т.д.;
- 7) Проведение анализа включенных, работающих сервисов;
- 8) Проведение сканирования:
 - поиск и анализ вирусов;
 - поиск и анализ артефактов программ для стеганографии;
- 9) Поиск, по ключевым словам:
 - составление списка ключевых слов;
 - формирование поискового запроса, с использованием синтаксиса выбранного поискового инструментария;
 - проведение поиска – целевого (в определенных директориях), всего пространства (включая нераспределенные области и удаленные разделы);

- составление отчета по результатам поиска;
- фильтрация данных (на основании метаданных – дата, время, расширение и т.д.);

На основном этапе исследования выполняются следующие действия:

1) Анализ данных.

Анализ файлов с использованием специализированного программного обеспечения. В качестве специализированного программного обеспечения может быть использован следующий экспертный инструментарий:

- анализ памяти;
- работа с паролями;
- интернет-активность;
- анализ e-mail сообщений;
- монтирование файлов-образов;
- работа с реестром ОС: Windows Registry Recovery – программа, предназначенная для анализа и редактирования реестра. Имеется возможность работы с реестром активной и пассивной ОС.

- восстановление данных;
- выявления ПО с признаками контрафактности.

2) Анализ основных областей.

Анализ основных областей выполняется для поиска артефактов и/или другой интересующей информации. Примером основных областей являются:

- рабочий стол;
- директория пользователя;
- директория «Документы»;
- директория «Загрузки»;
- директория «Недавние места»;
- временные директории браузеров;

3) Анализ системного реестра.

Анализ системного реестра помогает в получении важной информации как о самой системе, как о приложениях, так и об активности пользователя. Например:

- информация о последнем входе в систему
- имя пользователя и SID
- время последнего завершения работы
- носители, подключаемые пользователем
- установленное программное обеспечение

4) Анализ следов работы программного обеспечения: определение наличия программного обеспечения, анализ журналов (логов), настроек, реестра и т.д.;

5) Если есть возможность, то необходимо провести анализ временной информации, содержащейся в памяти.

6) Анализ переписки (e-mail, социальные сети).

Для анализа информации о переписке пользователя эксперту необходимо выполнить:

- Поиск установленных почтовых клиентов, архивов сообщений почтовых клиентов. Для анализа информации содержащейся в них используется либо почтовый клиент, либо специализированное программное обеспечение, предназначенное для просмотра файлов соответствующего типа;
- Поиск установленных программ обмена мгновенными сообщениями (QIP, ICQ и т.д.), архивов сообщений;
- Для анализа информации о переписке в социальных сетях (VK, Facebook, Twitter и т.д.) производится анализ интернет-активности пользователя;

7) Анализ интернет-активности.

Для анализа интернет-активности пользователя необходимо определить установленные браузеры и провести для них анализ артефактов, таких как:

- анализ файлов истории посещения (index.dat, sqlite и т.д.);
- анализ временных директорий;
- анализ куков (cookies);
- анализ кеша страниц;
- анализ избранного, закладок;
- анализ панели инструментов;
- анализ плагинов;
- анализ системного реестра;
- анализ удаленной информации.

В ходе проведения исследования, используемые методы фиксируются. В завершение экспертизы даются предварительные выводы, которые уточняются на последующих стадиях исследования¹.

Подводя итог, следует отметить, что использование электронных доказательств в расследовании преступлений, связанных с незаконным распространением наркотических средств, психотропных веществ и их аналогов, относительно недавно являлось новшеством. Однако, в настоящее время, это – перспективное направление в раскрытии и расследовании не только данного вида преступлений, но и других. В виртуальном пространстве все больше остается следов совершенных преступлений. Пропорционально этому растет и удельный вес электронных доказательств по уголовным делам. В связи с этим появляется своеобразная «гонка» правоохранительных органов и злоумышленников, в которой каждая из сторон старается применить новейшие информационные технологии. И в этом противостоянии правоохранительные органы обязаны находиться на шаг впереди, особенно при выявлении, собирании и исследовании электронно-цифровых доказательств для использования в изобличении субъектов преступлений.

Список литературы

1. Александрова М. В. Методика расследования преступлений, связанных с незаконным оборотом наркотических средств и психотропных веществ // Отечественная юриспруденция. 2017. № 10 (24). С. 51-53. Режим доступа: <https://cyberleninka.ru/article/n/metodika-rassledovaniya-prestupleniy-svyazannyh-s-nezakonnym-borotom-narkoticheskikh-sredstv-i-psihotropnyh-veschestv>.
2. Багмет А. М., Скобелин С. Ю. Извлечение данных из электронных устройств как самостоятельное следственное действие // Право и кибербезопасность. 2013. № 2. С. 22-27.
3. Земцова С. И. Участие специалиста в раскрытии и расследовании преступлений, связанных с незаконным оборотом наркотических средств, психотропных и сильнодействующих веществ: автореферат дис. ... кандидата юридических наук: 12.00.12. Москва, 2017. 26 с.
4. Коровин Н. К. Особенности расследования незаконного оборота наркотических средств с использованием сети Интернет // Международный научно-исследовательский журнал 2018. № 10 (76). Часть 2. С. 65-67.
5. Краткая характеристика состояния преступности в Российской Федерации за январь - сентябрь 2018 года // Официальный сайт МВД РФ [Электронный ресурс]. Режим доступа: <https://мвд.рф/reports/item/14696015>.

¹ Методические материалы по проведению компьютерно-технических экспертиз ФБУ Российского федерального центра судебной экспертизы при Министерстве юстиции Российской Федерации, 2014.

6. Криминалистика в 3 ч. Часть 2: учебник для вузов / Л. Я. Драпкин и др.; отв. ред. Л. Я. Драпкин. 2-е изд., перераб. и доп. М.: Издательство Юрайт, 2019. 230 с. (Серия: Бакалавр. Академический курс). ISBN 978-5-534-02040-3.
7. Овчинникова О. В. Собираение электронных доказательств, размещенных в сети Интернет // Правопорядок: история, теория, практика. 2016. № 4 (11). С. 67-70. Режим доступа: <https://cyberleninka.ru/article/n/sobiranie-elektronnyh-dokazatelstv-razmeshchennyh-v-seti-internet>.
8. Садырова М. С., Менжега М. М. Осмотр электронных устройств как самостоятельное следственное действие // Юридические науки: проблемы и перспективы: материалы IV Междунар. науч. конф. (г. Казань, май 2016 г.). Казань: Бук, 2016. С. 279-281. Режим доступа: <https://moluch.ru/conf/law/archive/181/10391/>.
9. Сафонов О. М. Уголовно-правовая оценка использования компьютерных технологий при совершении преступлений: состояние законодательства и правоприменительной практики, перспективы совершенствования: автореферат дис. ... кандидата юридических наук: 12.00.08. Москва, 2015. 22 с.
10. Судебная экспертиза: типичные ошибки / Е. И. Галяшина, В. В. Голикова, Е. Н. Дмитриев и др.; под ред. Е. Р. Россинской. М.: Проспект, 2012. 544 с.
11. Чернышов В. Н., Лоскутова Е. С. Проблемы собирания и использования цифровых доказательств // Социально-экономические явления и процессы. 2017. № 5. С. 199-203. Режим доступа: <https://cyberleninka.ru/article/n/problemu-sobiraniya-i-ispolzovaniya-tsifrovyyh-dokazatelstv>.
12. Чистанов Т. О. Незаконный сбыт наркотических средств с использованием телекоммуникационных сетей и устройств // Международный научно-исследовательский журнал. 2016. № 11. С. 86-88.

Nelli V. Racheva

Ph.D. Associate Professor
Ural State Law University
(Russia, Yekaterinburg)
ekaterinburgg@mail.ru

Yana V. Skorb

Student of Institute of State and International Law
Ural State Law University
(Russia, Yekaterinburg)
iana.skorb@gmail.com

MODERN TECHNOLOGIES OF COLLECTION AND RESEARCH OF ELECTRON-DIGITAL EVIDENCE IN THE INVESTIGATION OF CRIMES, CONNECTED WITH UNLAWFUL DEPRECTS OF DRUGS, PSYCHOTROPIC MATERIALS AND THEIR ANALOGUES

Abstract: The article discusses the main types of electronic digital evidence used in the investigation of crimes related to the illicit trafficking of narcotic drugs, psychotropic substances and their analogues. The concept of electronic digital evidence is formulated and a list of objects that can be attributed to such is given. The features and tactical methods of collecting electronic evidence relevant to the criminal case involving illicit drug trafficking are indicated. The article also presents the latest techniques and methods of computer-technical expertise.

Keywords: collection of evidence, admissibility of evidence, electronic-digital evidence, computer-technical expertise, electronic media, narcotic drugs.

Романов Алексей Николаевич

Кандидат юридических наук, доцент, доцент кафедры публичного права
Уральский государственный экономический университет
(г. Екатеринбург)
ran-mir@yandex.ru

Руколеев Виталий Александрович

Студент Института финансов и права
Уральский государственный экономический университет
(г. Екатеринбург)
v.a.rukoleev@bk.ru

**ПРОБЛЕМНЫЕ ВОПРОСЫ МЕХАНИЗМА ВЗАИМОДЕЙСТВИЯ СУДА С
ЛИЦАМИ, УЧАСТВУЮЩИМИ В СУДОПРОИЗВОДСТВЕ**

Аннотация: в данной статье рассматриваются проблемы электронного правосудия, как нового института процессуального права, в аспекте извещения участников процесса о времени и месте судебного заседания с использованием современных электронных средств и технологий. Автор анализирует действующее законодательство, приводит мнения отечественных ученых-юристов и на основе этого формулирует предложения по совершенствованию законодательства в области электронного правосудия.

Ключевые слова: электронное правосудие, судебное извещение, судебное заседание, электронная почта, сеть Интернет, электронные средства.

Развитие современных информационно-коммуникационных технологий коснулось всех сфер жизни общества. Не обошло стороной и судебную систему, где за последние годы был совершен большой прорыв в становлении нового института процессуального права в условиях информационного общества – электронное правосудие. Важным этапом в понимании механизма существования электронного правосудия стало принятие 26 декабря 2017 года Пленумом Верховного Суда РФ Постановления № 57 об использовании арбитражными судами и судами общей юрисдикции электронных документов¹. В акте разъяснены положения об электронном правосудии, которые касаются судов общей и арбитражной юрисдикции. В частности, разъяснены правила подачи документов в электронном виде, подготовки и рассмотрения дела с использованием документов в электронном виде, выполнения судебных актов в форме электронного документа, направления судебных актов и их образа в электронном виде, а также порядок извещений судами участников судебных заседаний. Но, помимо представленного судебного акта, дающего толкование и разъяснение правовых норм, регулирующих электронное правосудие как институт процессуального права, важно указать основополагающий нормативный правовой акт, положивший начало переходу к юридически значимому электронному документообороту в судах - Концепция федеральной целевой программы «Развитие судебной системы России на 2013 – 2020 годы»². Часть мероприятий, предусмотренных программой по созданию электронного правосудия, реализованы, а полученные результаты применяются в практической деятельности.

¹ О некоторых вопросах применения законодательства, регулирующего использование документов в электронном виде в деятельности судов общей юрисдикции и арбитражных судов: постановление Пленума Верховного Суда РФ от 26.12.2017 N 57 // Российская газета. N 297. 29.12.2017.

² Об утверждении Концепции федеральной целевой программы «Развитие судебной системы России на 2013 – 2020 годы»: распоряжение Правительства РФ от 20.09.2012 N 1735-р // Собрание законодательства РФ. 01.10.2012. N 40. Ст. 5474.

Само по себе электронное правосудие – это способ осуществления правосудия, основанный на использовании современных электронных средств и технологий. В юридической науке элементы электронного правосудия, в зависимости от их предназначения и направленности, подразделяются на три группы: элементы, отражающие открытость правосудия и судебной системы; элементы, направленные на обеспечение деятельности суда и его взаимодействие с другими государственными органами и органами местного самоуправления; элементы, направленные на взаимодействие суда с отдельными лицами, участвующими в судопроизводстве, по отдельным делам. Последний же элемент электронного правосудия, в части извещения участников процесса о времени и месте судебного заседания, вызывает наибольшее количество обсуждений в научных кругах.

В процессуальном законодательстве указывается, что суд может извещать о времени и месте судебного заседания лиц, участвующих в деле, с их согласия путем направления им извещений или вызовов по электронной почте (ч. 1 ст. 96 КАС РФ¹, ч. 4 ст. 1 ГПК РФ², ч. 5 ст. 3 АПК РФ³, ст. 232 УПК РФ⁴ в взаимосвязи с п. 7.1 Постановления Пленума Верховного Суда РФ от 22.12.2009 № 28 «О применении судами норм уголовно-процессуального законодательства, регулирующих подготовку уголовного дела к судебному разбирательству»⁵). Верховный Суд РФ решил, что такое согласие на извещение по электронной почте может быть выражено посредством указания адреса электронной почты в тексте обращения в суд, а также при подаче обращения в суд в электронном виде посредством заполнения соответствующей формы, размещенной на официальном сайте соответствующего суда в сети «Интернет». Предварительное согласие адресата на подобную рассылку, предусмотренное Федеральным законом «О связи»⁶, выраженного посредством совершения им действий, однозначно идентифицирующих этого абонента и позволяющих достоверно установить его волеизъявление на получение рассылки, не потребуется. Таким образом, при указании, например, в исковом заявлении адреса электронной почты истец соглашается получать извещения о судебных заседаниях именно на эту электронную почту. При этом, если суд располагает сведениями о том, что лицам известно о начавшемся процессе, то он может извещать их о времени и месте судебного заседания или совершении отдельных процессуальных действий, в том числе в судах апелляционной, кассационной и надзорной инстанций, путем размещения соответствующей информации на официальном сайте соответствующего суда в сети «Интернет». Но, в некоторых случаях суд обязан направлять извещения в бумажном виде. Например, если речь идет о назначении судебного заседания после принятия итогового судебного акта по делу, о принятии к производству заявления, представления о пересмотре судебного акта по новым или вновь открывшимся обстоятельствам или о восстановлении пропущенного срока подачи апелляционной (частной), кассационной, надзорной жалобы или представления.

По мнению А. А. Алексеева возможность использования электронной почты и соответствующих сайтов судов в сети «Интернет» для направления судебных извещений и

¹ Кодекс административного судопроизводства Российской Федерации от 08.03.2015 N 21-ФЗ (ред. от 27.12.2018) // Российская газета. 11.03.2015. N 49.

² Гражданский процессуальный кодекс Российской Федерации от 14.11.2002 N 138-ФЗ (ред. от 27.12.2018) // Парламентская газета. 20.11.2002. N 220-221.

³ Арбитражный процессуальный кодекс Российской Федерации от 24.07.2002 N 95-ФЗ (ред. от 25.12.2018) // Российская газета. 27.07.2002. N 137.

⁴ Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 N 174-ФЗ (ред. от 01.04.2019) // Российская газета. 22.12.2001. N 249.

⁵ О применении судами норм уголовно-процессуального законодательства, регулирующих подготовку уголовного дела к судебному разбирательству: постановление Пленума Верховного Суда РФ от 22.12.2009 N 28 (ред. от 15.05.2018) // Бюллетень Верховного Суда РФ. 2010. N 2.

⁶ О связи: Федеральный закон от 07.07.2003 N 126-ФЗ (ред. от 27.12.2018) // Российская газета. 10.07.2003. N 135.

вызовов вызывает сомнения в силу того, что зафиксировать факт получения письма адресатом невозможно, в отличие, например, от вручения расписки или заказного письма¹. И.М. Шевченко напротив отмечает, что извещение лиц, участвующих в деле, по адресу электронной почты допустимо в рамках арбитражного судопроизводства в силу его специфик². В этой связи им предлагается внести изменения в Федеральный закон «О государственной регистрации юридических лиц и индивидуальных предпринимателей»³ об обязательности указания в заявлении о государственной регистрации сведения об электронной почте юридического лица или индивидуального предпринимателя. В таком случае судебные извещения могут направляться юридическому лицу или индивидуальному предпринимателю только по адресу электронной почты.

Поддерживая мнения ученых-юристов, автор считает, что эффективность механизма доставки судебных извещений на адрес электронной почты лицам, участвующим в деле, вызывает сомнения. Несмотря на то, что данные меры предполагают оперативность в получении информации и возможности ее передавать, не учитывая местоположения адресата, следует принимать во внимание возможное отсутствие технической возможности доступа к сети «Интернет» в любом месте и в любое время. Например, в силу отсутствия подключения к сети «Интернет» в месте пребывания адресата или отсутствия у него технических средств доступа к сети «Интернет». Необходимо отметить и тот факт, что доставка сообщения по электронной почте может быть осложнена автоматическим размещением сообщения в локации массовых рассылок (спама). Также, следует обратить внимание на неопределенность в вопросе относительно того, с какого момента судебное извещение может считаться доставленным адресату и что считать надлежащим извещением. Размышляя над этими вопросами А. Х. Хисамов в своем научном труде предложил установить презумпцию надлежащего извещения по истечении определенного срока после направления извещения⁴. Не соглашаясь с приведенной точкой зрения, автор с целью решения рассматриваемой проблемы на законодательном уровне, обращается к проекту федерального закона «О внесении изменений в Гражданский процессуальный кодекс Российской Федерации», внесенного в декабре 2018 года на рассмотрение Государственной Думы Федерального Собрания (далее ГД ФС РФ) депутатами ГД ФС РФ⁵. Законопроектом предлагается установить порядок, при котором гражданин в случае имеющейся регистрации в федеральной государственной информационной системе «Единый портал государственных и муниципальных услуг (функций)» (далее Портал Госуслуг) и (или) на официальном сайте ФГУП «Почта России» (далее Почта России) сможет получать судебные извещения на представленных Интернет-ресурсах. При этом субъекты законодательной инициативы указали, что в обязанности Почты России добавляется необходимость извещения получателя судебного уведомления по адресу электронной почты. В тоже время в акте указывается, что данные меры не отменяют существующий порядок доставки судебных уведомлений, а лишь добавляют возможность информирования получателей. Подобная модель используется налогоплательщиками и налоговыми органами для реализации своих прав и обязанностей, предусмотренных налоговым законодательством. По общему

¹ Алексеев А. А. Электронное судопроизводство в российском гражданском процессе // Арбитражный и гражданский процесс. 2016. N 2. с. 14.

² Шевченко И. М. Извещение лиц, участвующих в деле, о времени и месте судебного разбирательства по делам о банкротстве // Судья. 2018. N 9. С. 62.

³ О государственной регистрации юридических лиц и индивидуальных предпринимателей: Федеральный закон от 08.08.2001 N 129-ФЗ (ред. от 27.12.2018) // Российская газета. 10.08.2001. N 153-154.

⁴ Хисамов А. Х. Тенденции интеграции информационных технологий в цивилистический процесс // Вестник гражданского процесса. 2018. N 1. с. 235-246.

⁵ Проект Федерального закона № 609507-7 «О внесении изменений в Гражданский процессуальный кодекс Российской Федерации», внесенный депутатами Государственной Думы В. К. Гартунгом, В. Г. Газзаевым, А. Н. Грешневиковым и другими // СОЗД ГАС «Законотворчество» [Электронный ресурс]. Режим доступа: <https://sozd.duma.gov.ru/bill/609507-7> (дата обращения: 18.05.2019).

правилу граждане уплачивают транспортный налог, земельный налог и налог на имущество на основании налогового уведомления, направляемого налоговой инспекцией. Уведомление может вручаться лично под расписку, пересылаться Почтой России заказным письмом, а также предоставляться в электронной форме через Личный кабинет налогоплательщика. Аналогичный механизм уведомлений граждан, например, о возбуждении исполнительного производства и о наличии штрафов за нарушение правил дорожного движения, предоставляется через опцию «Госпочта» на Портале Госуслуг.

Законопроект хоть и не получил одобрение Правового управления Аппарата ГД ФС РФ¹, но в целом предложенный механизм извещения адресатов о времени и месте судебного заседания традиционным образом путем отправки извещения почтовым отправлением с дополнительным информированием путем отправки уведомления об отправленном извещении почтовым отправлением на электронную почту и (или) на такие Интернет-ресурсы как Госуслуги и Почта России можно считать адекватной и эффективной мерой, направленной на совершенствование законодательства об электронном правосудии. Так, в случае нахождения гражданина вне места постоянной регистрации (например, в отпуске, в длительной командировке, в больнице и др.) есть вероятность, что он не сможет получить судебное уведомление в срок семь дней со дня доставки уведомления отделением почтовой связи в почтовый ящик, но будет дополнительно извещен при помощи электронных средств. В этом случае, получатель сможет своевременно явиться в отделение почтовой связи для получения извещения или проинформировать суд о невозможности получения извещения по объективным обстоятельствам.

Конечно, для того чтобы подобный механизм был законодательно закреплён требуется не только внесение изменений в федеральное законодательство (в числе которого Федеральный закон «О связи»), но и доработать некоторые положения самого законопроекта. Как пример, попытаться сформулировать предложения по применению описанного порядка направления судебных извещений в процессуальном праве в целом (парламентарии предусмотрели внесение изменений исключительно в ГПК РФ).

Список литературы

1. Алексеев А. А. Электронное судопроизводство в российском гражданском процессе // Арбитражный и гражданский процесс. 2016. N 2. С. 12-16.
2. Хисамов А. Х. Тенденции интеграции информационных технологий в цивилистический процесс // Вестник гражданского процесса. 2018. N 1. С. 229-247.
3. Шевченко И. М. Извещение лиц, участвующих в деле, о времени и месте судебного разбирательства по делам о банкротстве // Судья. 2018. N 9. С. 60-64.

Alexey N. Romanov

PhD in Law, Associate Professor,
Associate Professor of Department of Public Law,
Ural State University of Economics
(Russia, Yekaterinburg)
ran-mip@yandex.ru

Vitaly A. Rukoleev

Student of the Institute of Finance and Law
Ural State University of Economics

¹ Заключение по проекту Федерального закона № 609507-7 «О внесении изменений в Гражданский процессуальный кодекс Российской Федерации», внесенному депутатами Государственной Думы В. К. Гартунгом, В. Г. Газзаевым, А. Н. Грешневиковым и другими // СОЗД ГАС «Законотворчество» [Электронный ресурс]. Режим доступа: <https://sozd.duma.gov.ru/bill/609507-7> (дата обращения: 18.05.2019).

(Russia, Yekaterinburg)
v.a.rukoleev@bk.ru

PROBLEM ISSUES OF THE MECHANISM OF COURT INTERACTION WITH PERSONS INVOLVED IN LEGAL PROCEEDINGS

Abstract: this article deals with the problems of e-justice, as a new institution of procedural law, in the aspect of notifying participants of the process about the time and place of the court session using modern electronic tools and technologies. The author analyzes the legislation in force, cites the opinions of domestic legal scholars and, on the basis of this, formulates proposals for improving the legislation on e-justice.

Keywords: e-justice, court notice, court hearing, e-mail, Internet, electronic means.

Савоськин Александр Владимирович

Кандидат юридических наук, доцент,
советник судьи Уставного Суда Свердловской области,
доцент кафедры конституционного права
Уральский государственный юридический университет
(г. Екатеринбург)
savoskinav@yandex.ru

СТАНОВЛЕНИЕ В РОССИИ КОНСТИТУЦИОННОГО ПРАВА НА ОБРАЩЕНИЕ В СЕТИ ИНТЕРНЕТ

Аннотация. В статье анализируются два этапа становления и развития законодательства о подаче обращений граждан посредством сети Интернет: признание электронных обращений в качестве равнозначных к традиционным письменным (2006–2010 гг.) и дальнейшее развитие законодательства об электронных обращениях (с 2010 г. по настоящее время) связанное с появлением отдельных разновидностей электронных обращений граждан а также способов подачи электронных обращений: по электронной почте, посредством форм обратной связи официальных сайтов органов власти и универсальных порталов, посредством мобильных приложений.

Ключевые слова: право на обращение, электронное обращение, электронная почта, Интернет.

Развитие прогресса и прежде всего телекоммуникации поставило множество вопросов, связанных с правовым регулированием отношений, возникающих в сети Интернет и институт обращений граждан не стал исключением. Вместе с тем имеющееся законодательство об обращениях, подаваемых посредством электронных средств связи, отстает от реалий эпохи, демонстрируя несовершенство и пробельность правового регулирования в этой сфере.

Несмотря на крайнюю актуальность и востребованность информации об электронных способах подачи и рассмотрения обращений граждан, комплексные научные изыскания на эту тематику все еще отсутствуют, а имеющиеся публикации представлены только в периодических журналах и не отличаются глубиной проработки.

В развитии отечественного регулирования электронных обращений отчетливо прослеживается два этапа: первый – юридическое признание электронных обращений как равнозначных по отношению к традиционным письменным (2006–2010 гг.); второй – развитие законодательства об электронных обращениях, в том числе путем регламентации отдельных видов обращений, подаваемых исключительно посредством Интернет (с 2010 г. по настоящее время).

Впервые волеизъявления, выражаемые гражданами посредством телекоммуникационных систем, были признаны разновидностью обращений при принятии Федерального закона «О порядке рассмотрения обращений граждан Российской Федерации». Так, в ч. 3 ст. 8 была указано, что «обращение, поступившее в государственный орган, орган местного самоуправления или должностному лицу по информационным системам общего пользования, подлежит рассмотрению в порядке, установленном настоящим Федеральным законом». Никакой конкретизации этого положения, равно как и наименования разновидности таких обращений, законодатель не сформулировал, однако само упоминание электронных обращений в тексте закона стало отправной точкой в развитии законодательства о них. Федеральный законодатель приравнял электронные обращения к традиционным, но не раскрыл особенностей их подачи и рассмотрения. Можно сказать, что он лишь узаконил уже существующую

практику направления обращений посредством сети Интернет, но оказался не готов к подробному их регулированию. Эта и некоторые иные проблемы породили необходимость дальнейшего совершенствования законодательства об электронных обращениях, поэтому с 2010 года начинается качественно новый этап в развитии законодательства об обращениях, направляемых посредством сети Интернет, продолжающийся до сих пор.

В 2010 году ч. 3 ст. 8 Федерального закона «О порядке рассмотрения обращений граждан Российской Федерации» была существенно переработана¹ и дополнена термином «обращение в форме электронного документа», а п. 1 ст. 41 Арбитражного процессуального кодекса РФ был дополнен частью второй, предусматрившей право лиц, участвующих в деле, «представлять в арбитражный суд документы в электронном виде, заполнять формы документов, размещенных на официальном сайте арбитражного суда в сети Интернет»². Отмечу, что ч. 3 ст. 7 Федерального закона «О порядке рассмотрения обращений граждан Российской Федерации» были установлены следующие реквизиты электронных обращений: «фамилия, имя, отчество (последнее – при наличии), адрес электронной почты, если ответ должен быть направлен в форме электронного документа, и почтовый адрес, если ответ должен быть направлен в письменной форме». Показательно, что в отличие от привычных письменных обращений, в электронных обращениях *подпись и дата* не являются обязательными реквизитами. Это кардинально отличает подход отечественного законодателя от зарубежного, где отсутствие ЭЦП в электронном обращении гражданина – исключение из правила³. Причина такого подхода в исключительном (можно сказать избыточном) демократизме, который реализуя положения ст. 2 и 18 Конституции РФ о приоритете прав и свобод человека, обязал должностных лиц рассматривать фактически неподписанные электронные обращения. Однако у такого сверх демократического подхода оказались свои пределы и обращения в судах РФ принимаются либо при наличии ЭЦП, либо при условии представления образов документов подтверждающих личность заявителей в специальных личных кабинетах, создаваемых на официальных сайтах (например, Личный кабинет пользователя на официальном сайте Конституционного Суда РФ в сети Интернет <https://petition.ksrf.ru/>).

Отсутствие подписи заявителя в числе обязательных реквизитов и особенности виртуальной коммуникации (когда в сети Интернет можно зарегистрироваться под любым именем) еще более обострили существующую проблему анонимности обращений, ведь по меткому замечанию В.В. Комаровой «такое свойство сети «Интернет» как анонимность, вполне может оказать деструктивное влияние на развитие демократических процессов»⁴.

Думается, что в России уже начали складываться предпосылки к устранению имеющей фактической анонимности электронных обращений. Первый пример того, как это может быть сделано эффективно и без избыточных усилий для граждан, продемонстрирован Порталом государственных услуг – <http://www.gosuslugi.ru/>. Еще один интересный новейший пример демонстрирует Роспотребнадзор, а именно, с 1 января 2017 года запретивший проводить проверки по электронным обращениям граждан, если они поданы без авторизации заявителя в единой системе идентификации и аутентификации⁵.

¹ О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием Федерального закона «Об организации предоставления государственных и муниципальных услуг»: Федеральный закон от 27.07.2010 № 227-ФЗ (ред. от 03.12.2012) // СЗ РФ. 2010. № 31. Ст. 4196.

² О внесении изменений в Арбитражный процессуальный кодекс Российской Федерации: Федеральный закон от 27.07.2010 № 228-ФЗ // СЗ РФ. 2010. № 31. Ст. 4197.

³ См., например, специальный алгоритм направления электронных обращений, не подписанных ЭЦП, в полицию Казахстана. URL: <http://qamqor.gov.kz/EussWar>.

⁴ Комарова В. В. Электронная демократия – мифы и реальность // Ученые записки Худжанского государственного университета им. академика Б. Гафурова. Серия гуманитарно-общественных наук. 2016. № 3. С. 47.

⁵ О внесении изменений в Федеральный закон «О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля» и

Этот подход представляется очень интересным. Обращу внимание, что отсутствие подтвержденной идентификации заявителя не препятствует подаче обращения и его рассмотрению, однако его полезность для заявителя резко снижается, так как Роспотребнадзор не будет проводить проверок по факту обращения, а значит его ответ окажется, скорее всего, формальным и бесполезным. Таким образом создаются предпосылки стимулирования заявителей идентифицировать себя при подаче электронных обращений.

Вместе с тем, новейшее законодательство об электронных обращениях развивается экстенсивно, путем регламентации отдельных видов электронных обращений и способов их подачи. Приведем лишь основные новеллы федерального законодательства. Во-первых, следует упомянуть поправки 2011 года¹ к Федеральному закону «О предоставлении государственных муниципальных услуг», предусматривавшие создание Федеральной информационной системы досудебного (внесудебного) обжалования. Подзаконными актами к этому закону фактически введены *электронные досудебные (внесудебные) жалобы*. Во-вторых, следует назвать Указ Президента РФ, утвердивший правовой институт *общественной инициативы*, создавший особую электронную форму предложений, подаваемых исключительно на сайте «Российская общественная инициатива» – <https://www.roi.ru>². В-третьих, Кодекс административного судопроизводства РФ предусматривает с сентября 2016 года возможность подачи *всех* документов в суд в форме электронного документа³. В-четвертых, в последние годы во многих федеральных законах появились указания на возможность направления обращений в форме электронного документа, например, п. 4 ст. 1 и п. 1 ст. 7 Федерального закона «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления» и другие.

Что касается способов подачи обращений посредством сети «Интернет», то ни Федеральный закон «О порядке рассмотрения обращений граждан Российской Федерации», ни иной федеральный закон их не устанавливают. Однако в современной практике таких способов существует четыре. Первый и наиболее традиционный – направление обращения по электронной почте, второй – направление обращения через электронную приемную официального сайта адресата в сети Интернет, третий – посредством специализированных государственных интернет-порталов⁴; четвертый – посредством специальных официальных приложений для мобильных телефонов.

Согласно ч. 1 ст. 10 Федерального закона «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления» и ч. 1 ст. 10 Федерального закона «Об обеспечении доступа к информации о деятельности судов в Российской Федерации», все органы власти обязаны создать в сети Интернет свои сайты и адреса электронной почты. Однако какого-либо дополнительного регулирования законодатель не предложил, оставив его на усмотрение самих органов власти.

Еще более удручающей выглядит ситуация с направлением обращений через электронные приемные (интернет-приемные), или по-иному – формы обратной связи официальных сайтов в сети Интернет. Фактически электронная приемная – это встроенная в сайт подпрограмма, позволяющая заявителю направлять обращения, не пользуясь своей

Федеральный закон «О стратегическом планировании в Российской Федерации»: Федеральный закон от 03.07.2016 № 277-ФЗ // СЗ РФ. 2016. № 27 (ч. I). Ст. 4210.

¹ О внесении изменений в отдельные законодательные акты Российской Федерации: Федеральный закон от 03.12.2011 № 383-ФЗ (ред. от 24.11.2014) // СЗ РФ. 2011. № 49 (ч. 5). Ст. 7061.

² О рассмотрении общественных инициатив, направленных гражданами Российской Федерации с использованием интернет-ресурса «Российская общественная инициатива»: указ Президента РФ от 04.03.2013 № 183 (ред. от 23.06.2014) // СЗ РФ. 2013. № 10. Ст. 1019.

³ Ч. 2 и 3 ст. 45 Кодекса административного судопроизводства Российской Федерации от 08.03.2015 № 21-ФЗ (ред. от 19.07.2018) // СЗ РФ. 2015. № 10. Ст. 1391.

⁴ Более подробно см. Савоськин А. В. Специализированные официальные сайты в сети Интернет для подачи обращений граждан // Административное и муниципальное право. 2017. № 2. С. 84-94.

почтовой программой. Сформированное в электронной приемной обращение генерируется в виде обычного письма, поступающего на заранее указанный разработчиками сайта адрес электронной почты (как на официальный электронный адрес, так и любой другой). Здесь важно учитывать, что если электронная почта функционирует по единым во всем мире правилам, то электронные приемные – это «внутреннее» дело каждого сайта (соответственно, органа власти). При этом органы власти крайне редко стремятся нормативно закрепить соответствующие правоотношения, и нормы об электронных приемах носят явно разрозненный и бессистемный характер, поскольку федеральный законодатель не обязал органы власти создавать электронные приемные. Они появились как бы сами по себе под влиянием общих правил разработки сайтов программистами. Единственный федеральный акт (и то рекомендательного характера), предполагающий создание электронных приемных, – это Методические рекомендации по реализации принципов открытости в федеральных органах исполнительной власти¹.

Приложения для мобильных телефонов, позволяющие подавать обращения граждан появились относительно недавно. Например в мае 2014 года МВД России выпущено официальное приложение для мобильных устройств, которое в числе прочих возможностей позволяет совершить вызов ближайшего к месту нахождения абонента отдела полиции или направить электронное обращение в приемную министерства МВД России или территориальный орган внутренних дел². Подобные мобильные приложения являются довольно редким явлением в российской практике и увы, но их нормативное регулирование в свободном доступе отсутствует.

Первым общефедеральным порталом для подачи обращений в электронном виде стал Единый портал государственных и муниципальных услуг (функций) – <http://www.gosuslugi.ru/> который предоставляет целый комплекс возможностей для заявителей (от подачи заявлений до оставления отзывов, как особой разновидности обращений граждан), однако он касается не всех обращений граждан, а только подаваемых в связи с получением государственных и муниципальных услуг. Думаю, что с учетом позитивного опыта работы этого портал, а также интернет-портала досудебного обжалования предоставления государственных и муниципальных услуг (<https://do.gosuslugi.ru>), универсальных интернет-порталов для обращений граждан за рубежом и в отдельных субъектах Российской Федерации (например, единого сайта для подачи обращений граждан в Санкт-Петербурге <https://letters.gov.spb.ru>), пришло время учредить в России единый интернет-портал для подачи всех видов обращений, при этом предусмотреть три его подсистемы: федеральную, региональную и муниципальную. Такой интернет-портал не только станет еще одним способом подачи обращений, но и позволит гражданам отслеживать прохождение обращения в режиме реального времени (независимо от способа его подачи), а также будет являться инструментом мониторинга работы с обращениями и дополнительной гарантией их надлежащего и своевременного рассмотрения.

Список литературы

1. Комарова В. В. Электронная демократия – мифы и реальность // Ученые записки Худжанского государственного университета им. академика Б. Гафурова. Серия гуманитарно-общественных наук. 2016. № 3. С. 44–52.

¹ Методические рекомендации по реализации принципов открытости в федеральных органах исполнительной власти: утв. протоколом заочного голосования Правительственной комиссии по координации деятельности открытого правительства от 26.12.2013 № АМ-ПЗ6-89пр // Документ официально опубликован не был. Текст документа размещен на сайте. Режим доступа: <https://www.mintrans.ru/documents/9/3871> (дата обращения 18.05.2019).

² Официальный сайт мобильного приложения в сети интернет <https://приложения.мвд.рф>.

2. Савоськин А. В. Специализированные официальные сайты в сети Интернет для подачи обращений граждан // Административное и муниципальное право. 2017. № 2. С. 84-94.

Alexander V. Savoskin

PhD in Law, Associate Professor,

Advisor to the Deputy Chairman of the Charter Court of the Sverdlovsk region

Associate Professor of the Department of Constitutional Law

Ural State Law University

(Russia, Yekaterinburg)

savoskinav@yandex.ru

Abstract: The article analyzes two stages of the formation and development of legislation on electronic circulation: recognition of electronic circulation as equivalent to traditional written (2006–2010) and further development of legislation on electronic circulation (from 2010 to the present), the emergence of certain types of electronic communications appeals of citizens. The ways of submitting electronic messages are investigated: by e-mail, through feedback forms of official sites of authorities and universal Internet portals, through mobile applications.

Keywords: right to appeal, electronic appeal, e-mail, Internet.

Семис-оол Индира Сергековна
Студент Института юстиции
Уральский государственный юридический университет
(г. Екатеринбург)
Indira.semisool@mail.ru

«ЗАСЛУЖИВАЮЩИЙ ДОВЕРИЯ» ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ

Аннотация: В статье определяется актуальность темы искусственного интеллекта, о его потенциале существенного преобразования общества, анализируется понимание «заслуживающего доверия» искусственного интеллекта, раскрываются основные положения законности и этичности, как прозрачность, конфиденциальность, техническая устойчивость, приведен открытый перечень методов реализации «заслуживающего доверия» искусственного интеллекта, как правовое регулирование.

Ключевые слова: искусственный интеллект, этичность, «заслуживающий доверия», человек.

На сегодняшней день искусственный интеллект имеет высокий потенциал для существенного преобразования общества. Он является многообещающим средством повышения процветания человека, тем самым увеличивая индивидуальное и общественное благосостояние, а также принося прогресс и инновации. В частности, это касается решения вопросов изменения климата, рационализации использования природных ресурсов, улучшения качества образа жизни населения, в особенности в сфере здравоохранения, а также поддержка социальной сплоченности при намерении урегулировать данные проблемы. Для этого искусственный интеллект должен быть ориентирован на человека. Однако, предлагая большие возможности, также он может порождать и обратное, а именно определенные риски, оказывающие негативное влияние, в том числе воздействия, которые трудно предотвратить, например, на демократию, правосудие.

Об рисках было сказано уже в начале XXI века Стивеном Хокингом, что «сегодняшние достижения в области искусственного интеллекта поблекнут по сравнению с тем, что принесет следующее десятилетие. Успех в развитии искусственного интеллекта станет крупнейшим событием в истории человечества, поскольку искусственный интеллект может предоставить инструменты для искоренения войны, болезней и бедности.

Заглядывая в будущее, нет никаких фундаментальных ограничений для того, что может быть достигнуто, и возможен взрывной переход, хотя он может отличаться от того, что изображается в популярных журналах. Разработка искусственного интеллекта может привести к тому, что машины со сверхчеловеческим интеллектом перехватят финансовые рынки, перехитрят людей-исследователей, будут манипулировать лидерами-людьми и начнут разработки оружия, которое люди не смогут понять. Краткосрочное воздействие искусственного интеллекта зависит от того, кто его контролирует, но долгосрочное влияние зависит от того, можно ли вообще его контролировать.

Столкнувшись с потенциальным будущим неисчислимы выгод и рисков, было доказано, что эксперты не делают все возможное, чтобы обеспечить наилучший результат, и отмечают, что этим серьезным исследованиям посвящены некоторые некоммерческие институты. Они говорят, что все на местах должны спросить себя, что они могут сделать, чтобы повысить шансы пожинать плоды и избежать рисков».

Для того, чтобы избежать возможных рисков искусственный интеллект должен «заслужить доверие». А это, в свою очередь, означает что он должен согласовываться с

такими критериями, как, во-первых, законность, то есть соответствие закону, как, например, уважение достоинства личности, во-вторых, этичность, то есть обеспечение соблюдения этических принципов и ценностей, как, например, справедливость.

Эти два компонента в идеале должны взаимодействовать и гармонизировать друг с другом. Если на практике при взаимодействии возникает противоречие, то обществу следует обеспечить равновесие между ними.

Как и в случае с любой мощной технологией, использование искусственного интеллекта в нашем обществе порождает несколько этических проблем, например, связанных с их воздействием на человека и в целом на общество, на способность принятия решений и на безопасность. Если мы собираемся чаще использовать искусственный интеллект и делегировать им свои функции для решения возникших вопросов, то нам необходимо убедиться, что он справедлив в своем воздействии на жизнь людей, соответствует ценностям, которые не должны подвергаться риску.

При определении нормативного будущего искусственного интеллекта в Российской Федерации следует исходить из того, что система искусственного интеллекта должна основываться на этичности для того, чтобы она могла «заслужить доверие». Так, Южная Корея, которая является абсолютным лидером в использовании искусственного интеллекта предусматривает в своем национальном Законе о содействии развитию и распространению умных роботов в ст. 18 о возможности в будущем принять закон, регулирующий этические принципы в разработке, производстве и использовании робототехники и предусматривающий обязанность разработчиков, производителей и пользователей следовать указанным в нем положениям¹.

Для определения этичности «заслуживающего доверия» системы искусственного интеллекта опирается на основные права, закрепленные в Конституции РФ² и международных договорах РФ, как Конвенция о защите прав человека и основных свобод³.

Данные нормативные правовые акты закрепляют ряд фундаментальных прав, как равенство прав и свобод человека и гражданина. Эти права основаны на уважении человеческого достоинства, при котором человек обладает уникальными неотъемлемым статусом в гражданских, политических, экономических и социальных отношениях.

Человеческое достоинство включает в себе идею о том, что каждый человек обладает «внутренней ценностью», которая никогда не должна умаляться, подвергаться риску подавления, как человеком, так и системой искусственного интеллекта. В этом контексте уважение человеческого достоинства означает, что ко всем людям должно быть проявлено уважение, поскольку они являются субъектами права, а не объектом, которое можно продавать, манипулировать, сортировать. Таким образом, система искусственного интеллекта должна разрабатываться так, чтобы уважать и защищать неприкосновенность человека как его физическую, так и его психическую, и удовлетворять его основные потребности.

Человек должен оставаться свободным, чтобы принимать жизненные решения. В контексте искусственного интеллекта означает, что должно отсутствовать, например, необоснованное наблюдение, манипуляция людьми, влияние на психику человека. Свобода личности означает обязательство дать человеку возможность контролировать свою жизнь, включая использование таких прав, как свобода выражения мнения, право на частную жизнь.

¹ Закон о содействии развитию и распространению умных роботов: закон Южной Кореи № 9014 от 28.03.2008. Режим доступа: http://robopravo.ru/zakon_iuzhnoi_koriei_2008 (дата обращения: 18.05.2019).

² Глава 2. Права и свободы человека и гражданина // Конституция РФ. Режим доступа: <http://www.constitution.ru/10003000/10003000-4.htm> (дата обращения: 18.05.2019).

³ Конвенция о защите прав человека и основных свобод ETS № 005 Рим от 04.11.1950 г. Режим доступа: <https://base.garant.ru/2540800/> (дата обращения: 18.05.2019).

Также система искусственного интеллекта должна служить для поддержания и развития демократии, справедливости и верховенства закона. Они должны включать в себе обязательство не подрывать основополагающие принципы, на которых основано государство.

Так, этичность выражается в том, что система искусственного интеллекта не должна неоправданно подчинять, принуждать, обманывать, манипулировать, преследовать человека. Вместо этого они должны быть разработаны, чтобы расширять возможности человека. Распределение функций между системой искусственного интеллекта и человеком должно следовать принципу, ориентированному на человека и оставлять всегда возможность для человеческого выбора. Это означает обеспечение человеческого контроля над рабочими процессами в системах искусственного человека.

Также система искусственного интеллекта не должна причинять, не усугублять вред или иным образом оказывать неблагоприятное воздействие на человека. Особое внимание должно уделяться вследствие асимметрии власти, информации возможности контроля над искусственным интеллектом в противоправных целях.

В данном случае стоит упомянуть о технической устойчивости, которая требует, чтобы системы искусственного интеллекта разрабатывались превентивным подходом к рискам и, следовательно, вели себя как было задумано, минимизируя непреднамеренный и неожиданный вред.

Системы искусственного интеллекта, как и все программные системы, должны быть защищены от уязвимостей, которые могут использоваться злоумышленниками. Атаки могут быть направлены на заражение базы данных и утечку информации. И отсутствие должного уровня безопасности может привести к тому, что система возможно может принять неправильное решение, или полностью отключиться. А это в свою очередь может привести к неблагоприятным последствиям в виде ущерба.

Так, в случае возникновения проблем системы искусственного интеллекта должен быть запасной план как средство защиты от угроз. Это означает, что в процесс уже вступает человек-оператор, который направляет программу в нужном направлении. Необходимо убедиться, что система будет делать то, что должна, не причиняя вреда живым существам и окружающей среде.

Кроме того, должны быть установлены процессы для выяснения и оценки потенциальных рисков, связанных с системой искусственного интеллекта в различных областях применения. Требуемый уровень безопасности зависит от величины риска, создаваемого системой искусственного интеллекта, которая в свою очередь зависит от возможностей данной системы. Там, где возможно предвидеть, что процесс разработки и сама система искусственного интеллекта представляет высокий риск, то крайне важно, чтобы меры безопасности разрабатывались и опережали испытания.

Цели и возможности искусственного интеллекта должны открыто сообщаться. Прозрачность имеет решающее значение для создания и поддержания между разработчиками, производителями и пользователями системы искусственного интеллекта взаимодействия.

Для повышения прозрачности должны быть использованы такие меры, как возможность прослеживать, возможность проверять весь процесс при условии соблюдения системой основных прав. Особенно важно при выявлении ошибочных действий и дальнейшего совершенствования системы. Степень прозрачности также зависит от контекста и серьезности последствий или самой системы.

Равным образом, следует закрепить, что система искусственного интеллекта не должна представлять себя как человека при взаимодействии с человеком. Каждый имеет право получения информации о том, что они взаимодействуют с искусственным интеллектом. И при возможности необходимо предусмотреть отказ от диалога с ним в пользу общения с человеком.

Точность относится к способности системы искусственного интеллекта делать правильные суждения, например, для правильной квалификации информации по соответствующим категориям, или в ее способности делать правильные прогнозы, рекомендации или решения на основе имеющейся информации. В свою очередь, когда невозможно избежать случайных неточных предсказаний, важно, чтобы система могла указать насколько вероятны ошибки. Высокий уровень точности особенно важен в ситуациях, когда система искусственного интеллекта влияет на жизнь людей.

Вдобавок, должна быть обеспечена гарантия конфиденциальности и защиты данных на протяжении всего цикла работы системы. Это касается первоначальной информации, предоставленной пользователем, а также информации сгенерированную о пользователе в ходе взаимодействия с системой. Данные цифровые записи могут позволить искусственному интеллекту определять предпочтения отдельных лиц, но также и их сексуальную ориентацию, возраст, пол, религиозные и политические взгляды. Чтобы общество могло доверять ей, необходимо обеспечить, что собранная информация не использовалась в незаконных целях.

В равной степени, важно, чтобы присутствовала ориентированность на пользователя и была разработана так, чтобы все люди могли пользоваться продуктами и услугами искусственного интеллекта, в независимости от пола, расы, способностей.

Для обеспечения равного доступа к системе следует придать особое значение вопросам о возможности доступа людей с ограниченными возможностями, присутствующих во всех общественных группах.

При разработке «заслуживающего доверия» искусственного интеллекта желательно консультироваться с представителями общественных групп, чьи права и интересы могут затронуты.

При разработке, производстве и использовании возможно возникновение противоречий между вышеперечисленными положениями и для которых нет единого определенного решения. При их одинаковой важности необходимо учитывать их в контексте и с возможностями потенциальных разногласий между ними при применении в различных сферах.

Методы для реализации «заслуживающего доверия» искусственного интеллекта

Они могут взаимодополнять или быть альтернативным друг другу, поскольку в различных сферах имеется потребность в разных методах реализации. Потому как система постоянно развивается и действует в динамичной среде на постоянной основе должна проводиться их оценка:

1. Установление действий в виде создание белого и черного списка. В первом варианте должны быть предусмотрены правила, которым должна следовать система, а во втором варианте, которые никогда не должна нарушать. Если это касается системы искусственного интеллекта с возможностями обучения, то на первом этапе она должна распознавать все элементы окружающей среды, необходимые для обеспечения соблюдения требований, на втором этапе система должна рассматривать только, те планы, которые соответствуют требованиям, на последнем этапе действия должны быть ограничены поведение, которое реализует требования.

2. Разъяснение действий. Для того, чтобы система «заслуживала доверие», должно быть понимание почему она ведет себя определенным образом. Данный метод остается проблемой для систем искусственного интеллекта, основанных на нейронных сетях, так как небольшие изменения в значениях данных могут привести к значительным изменениям, что приведет к тому, что система, например, будет путать ребенка с собакой.

3. Тестирование. Данное действие должно проводиться как можно раньше, гарантируя, что система ведет себя так, как было задумано. Процессы тестирования должны разрабатываться и выполняться максимально разнообразной группой людей.

4. Правовое регулирование. Урегулирование данной сферы с помощью нормативных правовых актов, которые специально освещают систему искусственного интеллекта.

5. Управление. Создание определенных структур, обеспечивающие соответствие решений, связанных с разработкой, внедрением и использованием искусственного интеллекта, этическим аспектам, например, создание совета по этике.

6. Информированность. Поощрение взаимодействия между разработчиками, производителями и пользователями, и другими лицами, как, например, юристы, также возможность получения базовой грамотности или получения диплома специалиста в данной сфере.

Таким образом, крайне важно понимать, как наилучшим образом поддерживать разработку и использование искусственного интеллекта, чтобы каждый мог процветать в мире, основанном на передовых технологиях XXI века, и строить лучшее будущее.

Список литературы

1. Calo R. Robot Law / R. Calo, A. M. Froomkin, I. Kerr. Edward Elgar Pub, 2016. 424 p.
2. Ястребов О. А. Искусственный интеллект в правовом пространстве: концептуальные и теоретические подходы // Правосубъектность: общетеоретический, отраслевой и международно-правовой анализ: материалы XII Ежегодных научных чтений памяти С.Н. Братуся / ред. А. В. Габов. М.: Статут, 2017. 434 с.

Indira S. Semis-ool
Student of Institute of Justice
Ural State Law University
(Russia, Yekaterinburg)
Indira.semisool@mail.ru

TRUSTWORTHY ARTIFICIAL INTELLIGENCE

Abstract: The article determines the relevance of the topic of artificial intelligence, its potential for significant transformation of society, analyzes the understanding of trustworthy artificial intelligence, reveals the main provisions of legality and ethics, such as transparency, confidentiality, technical sustainability, provides an open list of methods for implementing trustworthy artificial intelligence as legal regulation

Keywords: artificial intelligence, ethical, trustworthy, person

Смахтин Евгений Владимирович
Доктор юридических наук, профессор,
профессор кафедры уголовного права и процесса
Института государства и права
Тюменский государственный университет
(г. Тюмень)
smaxt@yandex.ru

Зеленкина Ольга Юрьевна
Студент Института государства и права
Тюменский государственный университет (г. Тюмень)
o.zelenkina97@gmail.com

ТРАНСФОРМАЦИЯ ЭЛЕКТРОННО-ЦИФРОВЫХ СЛЕДОВ В ЭЛЕКТРОННО-ЦИФРОВЫЕ ДОКАЗАТЕЛЬСТВА: ВОПРОСЫ ТЕОРИИ И ПРАКТИКИ

Аннотация: В статье рассматриваются вопросы разработки и совершенствования технологии собирания, проверки и оценки электронно-цифровых доказательств. Раскрываются соотношения понятий «электронно-цифровые носители информации» и «электронные носители информации». Указывается на некоторые особенности обнаружения, фиксации, изъятия и исследования «виртуальных» следов. Рассмотрены некоторые вопросы использования криминалистически важной электронно-цифровой информации в качестве доказательств. В заключении, авторы обращают внимание на ряд практических проблем, связанных с использованием электронно-цифрового документооборота и электронных доказательств, как в рамках досудебного производства, так и в судебных стадиях.

Ключевые слова: электронный документооборот, электронно-цифровые носители информации, технические средства, электронные доказательства.

Вопросы модернизации Российской экономики, повышения качества принимаемых законов и эффективности их применения, напрямую связаны с цифровой или электронной информацией. Словосочетания «информация в электронной форме», «электронный документ», «электронная подпись» давно вошли в обиход, как ученых, так и практиков. Технологии стремительно проникают в нашу повседневную жизнь. Традиционная бумажная переписка практически полностью вытеснена электронной почтой, мессенджерами и социальными сетями. Это реальность, которую невозможно игнорировать.

Порядок использования электронных документов в уголовном судопроизводстве определен в Разделе XIX Уголовно-процессуального кодекса Российской Федерации (Федеральный закон от 23 июня 2016 г. № 220-ФЗ), предусматривающим электронный документооборот в информационно-телекоммуникационной сети «Интернет». С этого времени оборот электронных документов в виде ходатайств, заявлений, жалоб, судебных решений стал реальностью и в уголовном судопроизводстве.

Применительно к вещественным доказательствам законодатель использовал термин «электронные носители информации» (ст. ст. 81, 81.1, 82 УПК РФ и некоторые др.). В декабре 2018 Федеральным законом № 533-ФЗ Уголовно-процессуальное законодательство дополнено статьей 164.1 «Особенности изъятия электронных носителей информации и копирования с них информации при производстве следственных действий».

Как видим, в законодательстве России используется различная терминология. Применительно к перечисленным ранее понятиям в деловом обороте находятся, как обычные документы, так и электронные, а также электронно-цифровые документы. С технической точки зрения это разные документы. Представляется, что источниками цифровой информации могут служить не только электронные, но и иные устройства. В их числе, широко используемые сегодня информационные сети и системы, например, облачные сервисы и др.

Таким образом, можно сделать промежуточный вывод о том, что термин «электронно-цифровые носители информации» по объему шире, чем термин «электронные носители информации», который используется в уголовно-процессуальном законодательстве. Логично, что дальнейшее совершенствование уголовно-процессуального законодательства должно быть направлено на легализацию в законе термина «электронно-цифровые носители информации», что актуально для представителей процессуальной науки. Научные исследования, обосновывающие необходимость таких изменений, проводятся представителями уголовно-процессуальной науки¹.

Безусловно, электронный документооборот активно используется не только в регулируемом государством документообороте, но и преступниками. Возможность совершать противоправные действия, не имея непосредственного контакта с предметом преступления весьма привлекательна, поскольку помогает остаться не только не замеченным, но и не обнаруженным впоследствии. В качестве типичных предметов посягательств можно рассматривать электронные базы данных, серверы коммерческих организаций, государственных органов и учреждений, в том числе объектов критической информационной инфраструктуры РФ, банковские карты, электронные кошельки, электронные почтовые ящики, страницы в социальных сетях. Закономерно в электронных вычислительных машинах, информационно-телекоммуникационных сетях и информационных системах образуются специфические следы, которые чаще всего становятся единственной возможностью восстановить механизм преступления.

Технические и тактические вопросы работы с такими следами имеют определенную специфику. Разработка новых технико-криминалистических средств обнаружения, фиксации и изъятия таких следов, особенно учитывая, что последние могут модифицироваться, видоизменяться, уничтожаться представляется актуальным научным направлением в криминалистике.

Очевидно, что в уголовно-процессуальной и криминалистической деятельности все большее значение приобретают средства компьютерной техники, информационно-телекоммуникационные сети и информационные системы, которые позволяют повысить эффективность деятельности следователя и суда, а именно их функциональную составляющую, относящуюся к предметной сфере криминалистики.² Так, В. Б. Вехов предлагает термин «электронная криминалистика»³, однако не уточняет его соотношение с понятиями «электронная информация», «электронный документ» и др., что представляется не верным. Более точна, на наш взгляд, Е. Р. Россинская, методологически

¹ Засулин А. И. Правовые и методологические основы использования цифровой информации в доказывании по уголовному делу: автореф. дис. ... канд. юрид. наук. Екатеринбург, 2018. 32 с.

² См. напр.: Электронные носители информации в криминалистике: монография / под ред. О.С. Кучина. М.: Юрлитинформ, 2017. 304 с.; Бахтеев Д. В. Об алгоритмизации расследования и следственном мышлении // Проблемы современной криминалистики и основные направления ее развития в XXI веке: матер. межд. науч.-практ. конф. Екатеринбург: Издательский дом УрГЮУ, 2017. С. 48–54.

³ Вехов В. Б. «Электронная криминалистика»: понятие и система // Сборник трудов участников Международной научно-практической конференции. Ростов-на-Дону, 2017. С. 40–46.

обосновывающая теорию информационно-компьютерного обеспечения криминалистической деятельности¹.

Литература на эту обширную тему, хотя и многочисленна, носит неупорядоченный и фрагментарный характер. Возможности получения подобной информации большинству криминалистов-практиков неизвестны, и думается, что для успешной правоприменительной деятельности необходим особый комплекс специальных знаний, включающий в себя технологии собирания, проверки и оценки электронных доказательств. Научное обоснование такой необходимости также сформулировано процессуалистами, которые предлагают ввести такие термины в уголовно-процессуальное законодательство, как «технические средства», «электронные средства» и некоторые др.²

Криминалистика, являясь наукой, находящейся на передних рубежах противодействия преступности, изучает закономерности механизма совершения преступления и его отражения в материальных следах и идеальных образах. Вопросы обнаружения, фиксации, изъятия и исследования следов всегда находились в центре внимания криминалистов.

Передачу и хранение криминалистически значимой информации на современном этапе необходимо рассматривать не только для стационарных персональных компьютеров, их связи с локальными и глобальными сетями, но и для смартфонов, планшетных компьютеров, которые в силу своего всеобщего распространения в настоящее время являются одними из важнейших объектов криминалистического исследования, поскольку являются не только носителями и средствами передачи криминалистически значимой информации, но и предметами преступного посягательства, а также средствами совершения преступлений. Такие устройства уже не могут классифицироваться как ЭВМ, поскольку их работа во многом зависит от соединения с глобальной информационной сетью, а значит являются частью³. Они представляют собой интегрированные устройства, в которые входит персональный компьютер со специфическим программным обеспечением, устройство связи, носители информации (SIM-карты, карты памяти), глобальная система позиционирования (GPS), фото и видеокамеры.

Для квалифицированного изъятия электронных носителей информации и копирования с них информации при производстве следственных действий в соответствии со статьей 164.1 Уголовно-процессуального кодекса Российской Федерации во всех случаях необходимо участие специалиста. Каким бы уровнем компьютерных знаний следователь не обладал, скорее всего, их будет недостаточно для обнаружения и безошибочного изъятия следов преступления и обеспечения сохранности доказательств.

Подробное описание криминалистических технологий выявления, фиксации и изъятия криминалистически значимой информации при работе с компьютерными средствами и системами при производстве следственных действий должно содержаться в разделе криминалистическая тактика. Обратим внимание лишь на основные принципы, которыми следует руководствоваться при проведении следственных действий, сопряженных с изъятием компьютерных средств и систем.

По прибытии на место происшествия, не стоит пытаться самостоятельно проводить какие бы то ни было манипуляции с техникой, если результат заранее не известен. Кроме этого, следователь должен заблаговременно подготовить специализированные средства

¹ Россинская Е. Р. К вопросу о частной криминалистической теории информационно-компьютерного обеспечения криминалистической деятельности // Известия ТулГУ. Экономические и юридические науки. 2016. Вып. 3. Ч. II. С.110.

² Литвин И. И. Современные технические средства и проблемы их применения в доказывании на досудебных стадиях уголовного судопроизводства: автореф. дис. ... канд. юрид. наук. Екатеринбург, 2018. С. 9-10.

³ Семикаленова А. И., Сергеева К. А. Мобильные телефоны сотовой связи - новые объекты судебной компьютерно-технической экспертизы // Законы России, опыт, анализ, практика. 2011. № 12. С.89-94.

для изъятия виртуальных следов путем копирования – портативные криминалистические накопители, стандартные паспортизированные программы, предназначенные для копирования данных, с соответствующим документальным приложением, блокираторы записи, позволяющие предотвратить случайное или преднамеренное внесение изменений в данные, мобильную лабораторию. По ходатайству законного владельца изымаемых электронных носителей информации или обладателя содержащейся на них информации специалист осуществляет копирование изымаемых электронных носителей информации на другие электронные носители информации. Если специалист сделает вывод о том, что копирование информации может повлечь утрату или изменение информации, или иным образом может негативно отразиться на ходе расследования, копирование информации не допускается.

При отсутствии возможности проанализировать относимость доказательств к данному делу ввиду большого объема информации, отсутствии доступа или потенциальной опасности копирования информации, следователь вправе изъять электронное устройство, его часть, непосредственно содержащую информацию, а также несколько устройств, если они соединены между собой. При этом необходимо корректно завершить работу в строго определенной последовательности.

Обладая специальным программным обеспечением, сегодня мы можем получить криминалистически важную информацию путем удаленного доступа к устройству. Информация, полученная таким образом, может быть весьма полезна для следствия, однако вряд ли может быть признана доказательством, поскольку порядок ее процессуального оформления уголовно-процессуальным законодательством не регламентирован.

Помимо этого, интерес для криминалистики представляют тактика назначения и производства судебных компьютерно-технических экспертиз. В их числе можно назвать: судебную аппаратно-компьютерную экспертизу, судебную программно-компьютерную экспертизу, судебную информационно-компьютерную экспертизу данных. Еще одним видом является судебная компьютерно-сетевая экспертиза, объекты которой интегрированы из объектов перечисленных выше видов экспертиз, но лишь с тем отличием, что они все функционируют в определенной сетевой технологии. Еще одним видом экспертиз такого профиля являются экспертизы устройств сотовой связи.

В рамках, перечисленных выше экспертиз, на наш взгляд, может быть полезным использование единого специального криминалистического учета, в котором бы содержались ключи шифрования, данные о программно-техническом обеспечении и другая информация. Создание подобного учета может не только существенно облегчить процесс сбора и анализа статистических данных, но и представит новые возможности для идентификации, поскольку, по нашему мнению, программно-технические средства, создаваемые преступником самостоятельно, являются плодом высокоинтеллектуальной деятельности и практически также уникальны, как отпечатки пальцев.

Полагаем, что одной из задач криминалистики как науки является обеспечение перехода, трансформации следовой информации в доказательство. Взаимосвязь и различия уголовно-процессуальной и криминалистической деятельности очевидна. Термин «электронные доказательства» широко используется и в работах криминалистов, которые исследовали, как проблемы работы с электронными доказательствами, в условиях изменившегося уголовно-процессуального законодательства, так и особенности фиксации электронных доказательств¹. Авторы статьи разделяют позицию Д. В. Овсянникова, который считает, что компьютерная информация, полученная и проверенная в порядке, установленном уголовно-процессуальным законом, может стать доказательством. Этим же ученым обосновывается термин «электронное

¹ Вехов В. Б. Работа с электронными доказательствами в условиях изменившегося уголовно-процессуального законодательства // Российский следователь. 2013. № 10. С. 22-23.

доказательство»¹. По мнению В. С. Балакшина, результатом взаимодействия объектов материального мира является след в широком смысле этого слова, расшифровав который можно устанавливать обстоятельства, подлежащие доказыванию². Следовательно, первичен электронный след, который после соответствующей проверки может стать электронным доказательством.

Хотелось особо отметить, что провести четкую линию разграничения между предметами ведения криминалистики и уголовного процесса в вопросах, связанных с собиранием доказательств, авторы не планировали, поскольку это невозможно в рамках одной статьи. Хотелось лишь обратить внимание ученых и практиков на некоторые проблемы, возникающие при изучении одних и тех же объектов познания, и необходимость уточнения предметных сфер уголовного процесса и криминалистики.

В заключение отметим и другую тенденцию. Постоянное совершенствование системы электронного документооборота, безусловно, ведет к повышению качества оказываемых услуг, которые связаны с различными электронными сервисами. Современный мир стал очень мобильным, динамичным, что приводит и к повышению качества жизни. Однако на этом положительном фоне очевидно и другое. Перебои, сбои работы системы электроснабжения, напрямую связаны с отключением электронных сервисов, что в некоторых случаях приводит к парализации работы многих государственных учреждений («сбой системы», «упал Интернет», «сервис временно не доступен» и т.п.). Поскольку такие факторы могут оказывать негативное влияние на процесс расследования преступлений, задача криминалистики, в том числе разрабатывать алгоритмы действий следователя, в случае возникновения подобных ситуаций.

Список литературы

1. Балакшин В. С. Оценка допустимости доказательств в российском уголовном процессе: монография. М.: Юрлитинформ, 2016. С. 67.
2. Бахтеев Д. В. Об алгоритмизации расследования и следственном мышлении // Проблемы современной криминалистики и основные направления ее развития в XXI веке: матер. межд. науч.-практ. конф. Екатеринбург: Издательский дом УрГЮУ, 2017. С. 48–54.
3. Вехов В. Б. «Электронная криминалистика»: понятие и система // Сборник трудов участников Международной научно-практической конференции. Ростов-на-Дону, 2017. С. 40-46.
4. Вехов В. Б. Понятие, виды и особенности фиксации электронных доказательств // Расследование преступлений: проблемы и пути решения: сб. науч.-практ. тр. 2016. № 1. С. 155-158.
5. Вехов В. Б. Работа с электронными доказательствами в условиях изменившегося уголовно-процессуального законодательства // Российский следователь. 2013. № 10. С. 22-23.
6. Зазулин А. И. Правовые и методологические основы использования цифровой информации в доказывании по уголовному делу: автореф. дис. ... канд. юрид. наук. Екатеринбург, 2018. 32 с.
7. Литвин И. И. Современные технические средства и проблемы их применения в доказывании на досудебных стадиях уголовного судопроизводства: автореф. дис. ... канд. юрид. наук. Екатеринбург, 2018. С. 9-10.
8. Овсянников Д. В. Копирование электронной информации как средство уголовно-процессуального доказывания: автореф. дис. ... канд. юрид. наук. Екатеринбург, 2015. 21 с.

¹ Овсянников Д. В. Копирование электронной информации как средство уголовно-процессуального доказывания: автореф. дис. ... канд. юрид. наук. Екатеринбург, 2015. 21 с.

² Балакшин В. С. Оценка допустимости доказательств в российском уголовном процессе: монография. М.: Юрлитинформ, 2016. С. 67.

9. Россинская Е. Р. К вопросу о частной криминалистической теории информационно-компьютерного обеспечения криминалистической деятельности // Известия ТулГУ. Экономические и юридические науки. 2016. Вып. 3. Ч. II. С.110.

10. Семикаленова А. И., Сергеева К. А. Мобильные телефоны сотовой связи - новые объекты судебной компьютерно-технической экспертизы // Законы России, опыт, анализ, практика 2011. № 12. С.89-94.

11. Электронные носители информации в криминалистике: монография / под ред. О. С. Кучина. М.: Юрлитинформ, 2017. 304 с.

Evgeniy V. Smakhtin

Doctor of Law, professor,

Professor of Department of Criminal Law and Procedure,

The Institute of State and Law

Tyumen State University

(Russia, Tyumen)

smaxt@yandex.ru

Olga Y. Zelenkina

Student of the Institute of State and Law

Tyumen State University

(Russia, Tyumen)

o.zelenkina97@gmail.com

TRANSFORMATION OF ELECTRON DIGITAL TRACES INTO ELECTRON DIGITAL EVIDENCE: QUESTIONS OF THEORY AND PRACTICE

Abstract: The article discusses the development and improvement of technologies for collecting, researching and using electronic digital evidence. The author relates the concepts of «electronic digital information carrier» and «electronic information carrier». The article discusses the features of detection, fixation, removal and study of «virtual» traces. Some issues of using forensically important electronic digital information as evidence are considered. In conclusion, the author draws attention to a number of practical problems associated with the use of electronic digital documents and electronic evidence in enforcement activities.

Key words: electronic document management, electronic digital information carriers, technical means, electronic evidence.

Сысueva Елена Николаевна
Студент Института прокуратуры
Уральский государственный юридический университет
(г. Екатеринбург)
sysueva.lena@mail.ru

ВНЕДРЕНИЕ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА В ОРГАНЫ ПРОКУРАТУРЫ РФ

Аннотация: В данной статье освещен вопрос о том, что целесообразно создать в органах прокуратуры Российской Федерации единую систему электронного документооборота, которая бы включала в себя средства электронной почты, имеющие достаточную пропускную способность, единое пространство хранения документов (и карточек на них), доступное всем подразделениям органов прокуратуры. Рассмотрена стратегия развития отрасли информационных технологий в Российской Федерации на 2014 – 2020 гг. и на перспективу до 2025 г., которая определяет цели и основные направления развития указанной отрасли.

Ключевые слова: прокуратура, электронный документооборот, электронная подпись, стратегия развития отрасли информационных технологий.

Прокуратура Российской Федерации является ядром для совершенствования механизма взаимодействия органов исполнительной власти, направленного на недопущение и пресечение нарушений законности. Прокуратура как надзорное ведомство нуждается в своевременном обеспечении информацией, которое должно осуществляться непрерывно и в соответствующих объемах. Выполнение прокурорскими работниками своих профессиональных обязанностей сопряжено с непрерывностью получения (истребования) различной категории данных, а также их обработки и дальнейшего использования. Из этого вытекает, что развитие электронного документооборота и, следовательно, его правовое обеспечение является важным моментом работы и организации Прокуратуры Российской Федерации. Ввиду этого, рассмотрение в настоящей работе вопросов организации электронного документооборота в деятельности органов прокуратуры на сегодняшний день представляется весьма актуальным и востребованным.

Прежде чем начать более подробно разбираться с вопросом о необходимости внедрения и разработки электронного документа в работу органов прокуратуры, по моему мнению, для начала нужно разобраться с его теоретической составляющей.

Понятие «электронный документооборот» в Российском законодательстве не обозначено. Международное законодательство также не использует этот термин.¹ Поэтому попробуем сформулировать свое понятие. Насколько известно «электронный документооборот» является производным от «документооборота».

«Документооборот – движение документов с момента их получения или создания до завершения исполнения, отправки адресату или сдачи на хранение»². Соответственно, электронный документооборот – система, состоящая из множества процессов, связанных с движением, обработкой, получением и отправкой, а также хранением документов в электронном виде на электронном носителе.

¹ Шуваев А. Электронный документооборот как аналог традиционного // Бизнес консультант. 2008. № 12. С. 10.

² Феськова Т. Ю., Пустуев А. А., Рассохин А. В. Документационное обеспечение управления. Учебное пособие / под ред. А. Н. Митина. Екатеринбург: Издательский дом «Уральский государственный юридический университет», 2018. С.154.

В России существует стратегия развития отрасли информационных технологий в Российской Федерации на 2014 – 2020 гг. и на перспективу до 2025 г. Данная Стратегия определяет цели и основные направления развития указанной отрасли. Развитие электронного документооборота была названа одной из основных задач совершенствования отрасли информационных технологий в России и важнейшим внешним условием, необходимым для ее ускоренного развития.

Работа по развитию и внедрению электронного документооборота ведется различными государственными органами, в том числе органами прокуратуры Российской Федерации.

Рассмотрим преимущества и недостатки электронного документооборота в органах прокуратуры РФ. Внедрение Электронного документооборота позволит сократить издержки, упростить порядок взаимодействия, создать единое информационное пространство, возможность быстрой идентификации документа в системе, появится эффективная система отчетности, да и к тому же известно, что безопасность электронных документов выше, чем у документов на бумажном носителе. Восхваляя электронные системы документооборота, нельзя игнорировать и его слабые стороны: стоимостные затраты на его разработку, внедрение, совершенствование, но эти неизбежные расходы компенсируются значительной экономией времени и трудовых ресурсов; Высокая вероятность потери документов из-за вредоносного влияния вирусов или технических системных сбоев, в данном случае в качестве решения проблемы предлагаю создать электронную систему документорезервирования.

С учетом изложенного одним из важнейших направлений работы органов и организаций Прокуратуры Российской Федерации является развитие электронного документооборота и, соответственно, правовое обеспечение данного процесса.

Проведя анализ текущего состояния служебных процессов и информационных систем можно установить первоочередные потребности в автоматизации существующих служебных процессов прокуратуры и сформулировать предложения по оптимизации уже автоматизированных служебных процессов, в том числе по комплексному внедрению средств автоматизации. Принятые меры позволят в значительной мере перевести документооборот из бумажной формы в электронную и повысить эффективность деятельности органов прокуратуры.

Известно, что на сегодняшний день в органах прокуратуры РФ отсутствует единая система (платформа) электронного документооборота. Существует лишь программное автоматизированный информационный комплекс «Надзор» (далее – АИК «Надзор»), который был внедрен с целью систематизации и оптимизации документооборота. По моему мнению, данное программное обеспечение устарело. Кроме того, в нем отсутствуют многие необходимые функциональные возможности (например, коммуникации электронными сообщениями между работниками прокуратуры). Так же данная система действует не во всех подразделениях органов прокуратуры РФ и в некоторых прокуратурах до сих пор используются традиционные методы для регистрации бумажных документов – карточки, журналы и т.п.

Электронный документооборот является одним из необходимых условий для своевременного поступления (отправки) документов, обеспечивает сохранность и учет документов в органах прокуратуры, обмен информацией, передачу сведений о результатах деятельности прокуратуры в вышестоящие прокуратуры и иным лицам. В свою очередь, обеспечивает надлежащий уровень деятельности работников, а также полноту и своевременность решения поставленных перед органами прокуратуры задач.

Таким образом, в настоящее время целесообразно создать в органах прокуратуры Российской Федерации единую систему электронного документооборота, которая бы включала в себя средства электронной почты, имеющие достаточную пропускную способность, единое пространство хранения документов (и карточек на них), доступное всем подразделениям органов прокуратуры.

Невозможно не согласиться, что «в целях правового обеспечения функционирования единой системы электронного документооборота необходимо разработать и принять Положение «О единой системе электронного документооборота в органах и организациях прокуратуры Российской Федерации», учитывающее тенденции развития законодательства, регулирующего электронный документооборот, права, обязанности, ответственность всех участников информационного взаимодействия»¹.

При внедрении электронного документооборота следует поставить ряд задач: разработать требования к построению системы электронного документооборота, изменить внутреннюю систему управления деятельности органов прокуратуры, с учетом существующих наработок решить вопрос эффективного внедрения электронного документооборота.

Осуществляя выше поставленные задачи произойдет увеличение количества документов, создание и использование которых будет возможно в электронном виде, простая электронная подпись, усиленная неквалифицированная электронная подпись, а также подпись юридического лица будут более востребованы; использования отдельных электронных документов станет более удобным; повысится качественный и количественный результат работников органов прокуратуры, так же будет реализован принцип «одного окна».

Подводя итог всему сказанному, на мой взгляд, необходимо комплексно подходить к решению данного вопроса, поскольку с учетом большого объема работы органы прокуратуры нуждаются во внедрении и разработке электронного документооборота.

Список литературы

1. Феськова Т. Ю., Пустуев А. А., Рассохин А. В. Документационное обеспечение управления. Учебное пособие / под ред. А. Н. Митина. Екатеринбург: Издательский дом «Уральский государственный юридический университет», 2018.
2. Мышко Ф. Г., Кудряшов Е. Ю. Основные аспекты развития электронного документооборота в органах прокуратуры РФ. 2019.
3. Шуваев А. Электронный документооборот как аналог традиционного // Бизнес консультант. 2008. № 12.

Elena N. Sysueva

Student of Institute of Prosecutor's Office,
Ural State Law University
(Russia, Yekaterinburg)
sysueva.lena@mail.ru

INTRODUCTION OF ELECTRONIC DOCUMENTATION TO THE BODIES OF THE RUSSIAN PROSECUTOR'S OFFICE

Abstract: This article highlights the question of how it is expedient to create a single system of electronic document circulation in the prosecutor's offices of the Russian Federation, which would include the means of electronic mail, having sufficient throughput Ability, a single storage space of documents (and cards on them), accessible to all departments of the prosecutor's offices. The strategy of the Information technology industry development in the Russian Federation for 2014 – 2020 is considered. And for the future until 2025, which defines the goals and main directions of the development of the industry.

¹ Мышко Ф. Г., Кудряшов Е. Ю. Основные аспекты развития электронного документооборота в органах прокуратуры РФ. 2019.

Key words: Prosecutor's Office, electronic document circulation, electronic signature, strategy of development of Information Technologies Branch.

Холстинин Роберт Николаевич

Старший преподаватель кафедры философии и социологии
Уральский государственный юридический университет
(г. Екатеринбург)
holstinin11@yandex.ru

**ЦИФРОВЫЕ СИСТЕМЫ В ЧЕЛОВЕЧЕСКОМ ИЗМЕРЕНИИ. ВОПРОСЫ
РЕГУЛИРОВАНИЯ СЕТИ «ИНТЕРНЕТ».**

Аннотация: Вопросы регулирования сети «Интернет» сталкиваются с фундаментальным различием человеческого и машинного мышления. Человеческое мышление оперирует «смыслами», «содержанием». Машинное мышление – формальной структурой языка. Поэтому регулирование «содержания» сайтов в сети «Интернет» затруднительно или вызывает нежелательные последствия, поскольку осуществляется на основании «машинной» логики.

Ключевые слова: Регулирование сети «Интернет», машинное мышление, человек.

Под цифровыми системами мы будем понимать симбиоз человека и машины или системы машин, для выполнения некоторых «человеческих» задач. Примерами таковых можно привести сеть «Интернет», отдельные сайты этой сети, а также технические устройства, предназначенные для их функционирования.

Вопросы цифрового развития, применения информационных технологий сейчас обладают несомненной актуальностью. Однако, часто эти вопросы становятся «модой», показателем псевдо-современности исследования. Не упомянув «большие данные», «распределённый реестр» или «искусственный интеллект» легко прослыть ретроградом.

«Цифровые технологии» призваны улучшать *человеческую* жизнь, решать *человеческие* проблемы. Сейчас эти технологии развиваются из собственной логики и *человеческие* потребности являются лишь декларацией и побочным продуктом. Зачем «умным» гаражным воротам платные СМС-рассылки?¹ Многим знакома ситуация, когда мобильный телефон «сходил в интернет» в «чужом» регионе, а пользователь получил огромный счёт. «Цифрофизация» зачастую проводится ради самой «цифровизации». Там, где нет формальных математических и логических моделей компьютер превращается в средство решения вспомогательных задач. Самое простое – это использовать компьютер как печатную машинку для написания отчётов. Внедрение «цифры» - рай для бюрократа. Цифровые продукты наглядны и поддаются учёту. Они, якобы, «беспристрастны», но, в то же время, решают какую-нибудь побочную «бюрократическую» задачу. Комплексы видеофиксации нарушений ПДД призваны «приучить» водителей соблюдать скоростной режим, но заодно, являясь весомым источником пополнения местных бюджетов. Какая задача приоритетнее? Ответ не очевиден.

Есть более общий вопрос: чем руководствоваться при «цифровизации» той или иной гуманитарной области – «логикой средств» или «логикой содержания»? Сейчас существует существенная зависимость «цифровизации» от *наличной* вычислительной техники и *наличного* программного обеспечения. И задачи ставятся именно исходя из их возможностей в ущерб «формализуемой» области. Так ли актуальна задача создания беспилотного автомобиля? Или эта задача решается уже сегодня теми средствами, что уже есть и будет хорошо продаваться на рынке. Приоритету «логики средств», на наш взгляд,

¹ «... собеседник радиостанции однажды прославился историей, когда установил сим-карту на свои автоматические ворота на даче. После этого ворота самостоятельно подписались на платные СМС-рассылки». <https://www.bfm.ru/news/413647>.

способствуют такие основные причины как «нестабильность» компьютерных технологий и изменение алгоритмических языков и языков программирования. К тому же, формализация имеет теоретические пределы, очерченные теоремой Гёделя¹.

Человек в своём мышлении оперирует «смыслами», а машина «формальной» структурой языка. Отсюда вытекает необходимость различения логического следования и убедительности рассуждения. Есть известный софизм: «Если суждено умереть, то даже если вызвать врача – умрёшь, а если не суждено умереть, то даже если не вызвать врача, то не умрёшь. В любом случае вызывать врача бессмысленно». Формализовав данный софизм можно без труда убедиться, что полученная формула не является «логическим законом». На этом формальное опровержение обычно кончается. Однако, софизм истинен, например, при условии, что и «умереть суждено» и «врача вызвал», но «не умер»??? Человеческое мышление опровергая этот софизм будет утверждать, что «вызывать врача не бессмысленно», т. е. апеллировать к содержательной стороне рассуждения. «Машинное» мышление будет апеллировать к тому, что из этих посылок данное заключение не следует. Есть ещё и прагматический контекст этого рассуждения. Оно является переформулировкой рассуждения из Корана (Сура № 3, 145 аят). Для мусульманина *что* будет являться опровержением? Формальное рассуждение допускает бессмысленные и абсурдные высказывания, человек этого избегает («Если идеи зелёные, то автор этой статьи Наполеон» - истинное высказывание). Конъюнкция коммутативна, человеческие высказывания, построенные с использованием этого логического союза коммутативны не всегда. Нельзя поменять местами высказывания во фразе «Съел пирожок и умер». «Умер и съел пирожок» возможно только для машины, но не для человека. Примеры различий можно множить.

Где та граница, до которой можно допускать машинное мышление в человеческую жизнь? Опрос компании HeadHunter показал, что у 11% россиян роман завязался в интернете². Не обрушат ли торговые роботы фондовый рынок с катастрофическими последствиями для реальной экономики? Стимулируют ли «умные» системы к легальному поведению самого человека³? Автор этой статьи, рассматривая систему доказательственного права, показал, что «Модный в последнее время процессуальный технологизм, граничащий с банальным упрощенчеством (урезанное судебное следствие один из примеров тому) в итоге все дальше уводит судопроизводство от установления истины. Вместе с тем, правосудие, оторванное от истины, перестает быть правосудием»⁴. Технологизм это как раз и есть пример машинного мышления. «Электронный судья» должен будет устанавливать истину. А что есть истина? «Соблюдение законов логики дает эффект лишь при оперировании с теми или иными суждениями, почерпнутыми из полученных по делу доказательств, которые могут неадекватно отражать действительность. Чем же тогда измерить «метафизическую» (по Н. А. Бердяеву) истинность выводов органов следствия и суда?

Единственно возможный ответ – мерило истинности – внутреннее убеждение. Эта позиция закреплена в действующем УПК Российской Федерации. Его ст. 17 гласит: «Судья, присяжные заседатели, а также прокурор, следователь, дознаватель оценивают доказательства по своему внутреннему убеждению, основанному на совокупности имеющихся в уголовном деле доказательств, руководствуясь при этом законом и совестью». В этой части кодекс не поменялся, сохранив определенную преемственность

¹ Э. Мендельсон. Введение в математическую логику. М. 1971 г. С. 158 и далее.

² Эксперты рассказали, какие знакомства чаще всего завершаются свадьбой // РИА Новости [Электронный ресурс]. Режим доступа: <https://ria.ru/20120706/693275007.html> (дата обращения 18.05.2019).

³ DEX страдают от вредоносных торговых ботов // CoinDuck [Электронный ресурс]. Режим доступа: <https://coinduck.ru/articles/blog/dex-stradayut-ot-vredonosnykh-torgovykh-botov/> (дата обращения 18.05.2019).

⁴ Софронов Г. В., Холстинин Р. Н. Стремление к истине как доминанта развития уголовно-процессуального доказательственного права. Российский юридический журнал. 2019. № 2.

со статьей 71 УПК РСФСР 1960 года»¹. Возможно ли сформировать «внутреннее убеждение», а тем более «совесть» у электронного правосудия? Автор ни в коем случае не принадлежит к современным луддитам. Не стоит бояться «умного холодильника» даже в кооперации с «умным чайником»². Однако здесь есть вопросы требующие обсуждения.

Ещё одной проблемой, вытекающей из взаимодействия человека и машины, является опасность снижения профессиональной квалификации пользователя специалиста. Какое время необходимо для подготовки судьи? Нормативно, около 10 лет. И потом, непрерывный процесс самосовершенствования. В случае же ситуации, когда многие человеческие действия выполняет некая система, у человека может возникнуть впечатление, что ему самому не надо самосовершенствоваться. Реальной становится возможность появления неквалифицированного специалиста. Выявить его невысокую квалификацию затруднительно. Однако, рано или поздно встретится нестандартная ситуация, не учтённая системой предписаний. При неквалифицированном пользователе цифровизация не уменьшает вероятность ошибок, а увеличивает их масштаб и последствия, что доказали катастрофы самолётов последнего времени.

Естественно, что такая ситуация нуждается в регулировании. Сегодня регулирование в сети интернет происходит далеко не лучшим образом. Текущая нормативная база для блокировки Роскомнадзором (речь о требовании Генеральной Прокуратуры № 27-31-2018/Ид2971-18³) о «принятии мер к ограничению доступа к информационным ресурсам») используется для веерных блокировок ресурсов и сервисов, при этом страдают честные пользователи.

В апреле 2018 попытка соблюсти законное решение суда по блокировке мессенджера Telegram привело к тому, что в Реестр запрещённых сайтов было внесено 16,3 млн. IP адресов. В результате сильно пострадали многие сервисы и сайты, находящиеся физически как в России, так и за рубежом (много IP адресов располагалось на крупнейшем американском хостинге Amazon, а на нём сайты многих СМИ и интернет-сервисов, в том числе и Telegram). Более того, пострадали сервисы, которые отвечают за безопасность в целом: сервисы обновления Microsoft (в том числе критические обновления), онлайн-банк «Сбербанк» для мобильных устройств, и даже платежный шлюз 3D Secure MasterCard (что повлекло за собой невозможность проводить онлайн-платежи)⁴. Желание во что бы то ни стало заблокировать Telegram повлекло за собой существенные убытки у многих сайтов.

Налицо конфликт: вынесено решение о блокировке, но технически оно неисполнимо в полной мере. До сих пор мессенджер Telegram хоть и с некоторым затруднениями работает в Российской Федерации (стикеры в приложении стали грузиться медленнее). И отсюда встаёт вопрос, когда нужно прислушиваться к юристам, а когда к программистам?

Текущая нормативная база по регулированию в сети интернет не состыкуется с реальностью и техническими возможностями блокировать нежелательное содержание сайтов.

Текущая система регулирования «контента» в сети интернет основана на ограниченном списке IP адресов и доменов. Проверить доступ к ресурсу можно здесь <https://blocklist.rkn.gov.ru>. В настоящий момент в Реестре запрещённых сайтов находится

¹ Софронов Г. В., Холстинин Р. Н. Стремление к истине как доминанта развития уголовно-процессуального доказательственного права. Российский юридический журнал. 2019. № 2.

² Mr. Чайник. Сбербанк // Youtube [Электронный ресурс]. Режим доступа: https://www.youtube.com/watch?time_continue=188&v=7AtNPSRyU0Y (дата обращения 18.05.2019).

³ Документ с сайта Международной правозащитной группы Agora [Электронный ресурс]. Режим доступа: https://agora.legal/fs/a_delo2doc/90_file_Trebovanie_Genprok_RKN.pdf (дата обращения 18.05.2019).

⁴ Список сервисов и сайтов, которые стали жертвами блокировки Telegram // AKKet.com [Электронный ресурс]. Режим доступа: <https://akket.com/raznoe/96616-spisok-servisov-i-sajtov-kotorye-stali-zhertvami-blokirovki-telegram-v-rossii.html> (дата обращения 18.05.2019).

примерно 997 000 уникальных IP адресов (из записей с типом блокировки «по IP-адресу», данные от 12 мая 2019 года).

Список пострадавших и деградировавших сервисов в России уже довольно большой. Просто для понимания масштабов проблемы, заблокированы или сильно деградированы по качеству некоторые инфраструктурные сервисы:

- Slack¹ – корпоративный мессенджер.
- TeamViewer² — ПО для удалённого доступа.
- DigiCert³ - утилиты для проверки SSL-серверов.
- NTP-сервера проекта pool.ntp.org.⁴
- сервер обновлений и API сетевого оборудования Netgear.⁵
- архиватора WinRAR.⁶

Деградировали некоторые банковские сервисы:

- Банк Канады.⁷
- API российского банка Tinkoff.⁸

Некоторые СМИ:

- Wire.⁹
- французский Le Monde.¹⁰
- американский Politico.¹¹
- британский The Guardian.¹²
- BBC¹³ и других.

Если зайти на многие из этих ресурсов, вы как пользователь, можете получить от сайта или сервиса IP адрес из заблокированного диапазона. И это только некоторые из самых известных сервисов и сайтов, но полный список их огромен¹⁴.

При этом нужно понимать, что IP адрес – это не собственность, один раз закреплённая за сайтом или сервисом, а скорее аренда и IP адреса периодически меняют своего владельца. Существует пять RIR: ARIN, обслуживающий Северную Америку; APNIC, обслуживающий страны Юго-Восточной Азии; AfriNIC, обслуживающий страны Африки; LACNIC, обслуживающий страны Южной Америки и бассейна Карибского моря; и RIPE NCC¹⁵, обслуживающий Европу, Центральную Азию, Ближний Восток. Региональные регистраторы получают номера автономных систем и большие блоки адресов у IANA¹⁶, а затем выдают номера автономных систем и блоки адресов меньшего размера локальным интернет-регистраторам (Local Internet Registries, LIR), обычно являющимся крупными провайдерами.

¹ mpmulti-7glu.lb.slack-msgs.com и everything.lb.slack-msgs.com — 13.230.65.47 и 13.231.156.136 (13.230.0.0/15)

² trust.teamviewer.com — 13.58.128.219 и 18.218.93.240 (13.56.0.0/14, 18.218.0.0/16)

³ ssltools.digicert.com — 54.213.205.41 (54.212.0.0/15)

⁴ ntp-sin-02.no-such-agency.net — 167.99.64.239 (167.99.0.0/16)

⁵ updates1.netgear.com — 34.241.19.122, 34.243.216.129 (34.240.0.0/13)

⁶ ns2.win-rar.com — 174.138.9.247 (174.138.0.0/17)

⁷ bankofcanada.ca — 34.243.56.93 (34.240.0.0/13)

⁸ 2018-api.tinkoff.ru — 34.251.46.176 (34.248.0.0/13)

⁹ wire.com — 34.251.18.112 (34.248.0.0/13)

¹⁰ lemonde.fr — 195.154.120.129 (195.154.0.0/17)

¹¹ www.politico.eu — 35.177.248.225, 35.177.52.163 (35.176.0.0/15)

¹² advertising.theguardian.com — 35.177.35.0 (35.176.0.0/15)

¹³ buzz-cms.int.tools.bbc.co.uk — 34.249.84.78 (34.248.0.0/13), 54.229.156.84 (54.228.0.0/15)

¹⁴ Роскомнадзор vs Telegram: Список жертв // ihodl.com — иллюстрированное издание о криптовалютах и финансовых рынках [Электронный ресурс]. Режим доступа: /https://ru.ihodl.com/analytics/2018-04-18/roskomnadzor-vs-telegram-spisok-zhertv/ (дата обращения: 18.05.2019).

¹⁵ https://www.ripe.net

¹⁶ https://www.iana.org

Но как распорядиться самими IP адресами – это дело их владельца (в том числе хостинг компании). Сложно представить более абсурдную ситуацию, когда вы открываете свой персональный блог на каком-нибудь известном хостинге, но оказывается, что IP адрес вашего сайта был внесён в список заблокированных. Причём доказать, что на вашем IP адресе уже нет «запрещённого контента» на порядок сложнее, чем в него попасть.

Ещё не менее абсурдные ситуации складываются тогда, когда из-за одного заблокированного элемента на том или ином ресурсе, блокируется весь ресурс. Из последних примеров можно привести то, что Last.fm заблокирован в России из-за одной песни¹, поскольку ресурс работает по протоколу https, то блокировка страницы с песней привела к неработоспособности в России всего ресурса.

Совершенно очевидно, что текущую схему регулирования интернета необходимо менять, как с правовой точки зрения, так и с технической.

С правовой точки зрения видится, что необходимо уходить от практики формального наличия незаконного «контента», а разбираться индивидуально с каждым ресурсом. С технической точки зрения видится, что необходимо уходить от массовой блокировки ресурсов по IP адресу, поскольку страдают другие полезные сайты и сервисы.

Тут можно посмотреть на опыт других стран, как у них обстоят дела с регулированием интернета. В КНР, несмотря на наличие проекта «Золотой щит» (а если упрощённо, то «Великого Китайского Фаервола»)², властями Китая заявлено, что никаких внешних «нежелательных» ресурсов не будет показываться гражданам Китая. Для Китая есть специальная версия Yahoo и многих других мировых СМИ и сайтов, заблокированы все популярные социальные сети Instagram, Twitter, Facebook, Youtube, и др. Все заблокированные сайты тем не менее доступны через VPN и другие сервисы³. И тем не менее, китайских граждан не сильно беспокоит блокировка внешнего интернета, поскольку для обмена информацией повсеместно используется приложение WeChat, поскольку сочетает в себе лучшие качества мессенджера, соцсети, приложения с видео- и аудиозвонками, платёжной системой WeChat Pay и многими другими функциями. Тем самым, получается можно комфортно жить и без полноценного доступа во внешний интернет. Но у данного решения есть один существенный минус – очень медленный интернет и плохая связанность сети.

Другой пример – Нидерланды. В этой стране вообще нет как такового регулирования интернета, и по факту никакой фильтрации трафика не производится, законодательство абсолютно либерально относится к информации и её распространению. В 2012 году операторы начали блокировать «нарушения авторских прав». В январе 2012 года интернет-провайдеры Ziggo и XS4ALL по решению суда (по делу Bescherming Rechten Entertainment Industrie Nederland (BREIN)) – были обязаны заблокировать веб-сайт «The Pirate Bay». Не все были согласны на это и начались суды по этим вопросам. Некоторые провайдеры блокировали веб-сайт «The Pirate Bay», а некоторые нет, среди тех, кого суд обязал блокировать были: KPN, UPC, T-Mobile и Tele2. В итоге, Нидерланды стали одной из первых стран в мире, где понятие Net Neutrality (сетевой нейтралитет) законодательно закрепили – 4 июня 2012 года⁴.

Сетевой нейтралитет – принцип, по которому провайдеры телекоммуникационных услуг не имеют права фильтровать трафик, за исключением четырёх случаев:

¹ Пользователи Last.fm сообщили о блокировке сервиса в России // РБК.ru [Электронный ресурс]. Режим доступа: https://www.rbc.ru/technology_and_media/02/05/2019/5ccad1399a79475f5e32bdd1 (дата обращения 18.05.2019).

² Проект «Золотой щит» // Википедия – свободная энциклопедия [Электронный ресурс]. Режим доступа: https://ru.wikipedia.org/wiki/Золотой_щит (дата обращения 18.05.2019).

³ Я обхожу интернет-блокировки в Китае // The Village [Электронный ресурс]. Режим доступа: <https://www.the-village.ru/village/business/opyt/309909-internet-v-kitae> (дата обращения: 18.05.2019).

⁴ Нидерланды приняли закон о сетевом нейтралитете // Хабр [Электронный ресурс]. Режим доступа: <https://habr.com/ru/post/284724/> (дата обращения: 18.05.2019).

1. Судебное постановление или требование закона.
2. Согласие конечного пользователя.
3. Обеспечение целостности и безопасности сети или компьютера пользователя (с предварительным уведомлением пользователя).
4. Минимизация «заторов» в сети, в этом случае одинаковые типы трафика должны расцениваться равнозначно.

Принятие закона об Net Neutrality (ст. 7а Закона о телекоммуникациях) привело к тому, что операторы воспротивились требованию закона, которое могло бы привести к обязательной установке на сетях операторов систем DPI и анализа трафика. В результате общество воспротивилось принятию интернет регулирования, и оно было полностью отменено.

Если вернуться к России, видно, что государство пытается навести порядок в законах о интернете, о чём свидетельствует принятие закона «О суверенном интернете»¹. Несмотря на все опасения экспертов, по закону не будет блокироваться интернет (в китайском варианте), кроме как случаев чрезвычайной необходимости или необходимости защиты цифровых рубежей России. Но ситуация с регулированием явно требует изменений как в правовой, так и технической точки зрения. Даже внедрение полного DPI анализа трафика в России не решит проблемы с технической стороной блокировок.

Президент Владимир Путин в своем послании Федеральному собранию 20 февраля 2019 года призвал «настроить законодательство на новую технологическую реальность», и потребовал принять законы, которые не будут мешать «цифровой экономике»². Совершенно очевидна правильность этих решений, но тем не менее актуальность регулирования интернета и принятия новых, адекватных технической реализуемости законов в этой области необходима.

Robert N. Holstinin

Senior Lecturer of the Department of Philosophy and Sociology,
Ural State Law University
(Russia, Yekaterinburg)
holstinin11@yandex.ru

DIGITAL SYSTEMS IN HUMAN DIMENSION. INTERNET REGULATION ISSUES

Abstract: the Issues of regulation of the Internet are faced with a fundamental difference between human and machine thinking. Human thinking operates with «meanings», «content». Machine thinking is the formal structure of language. Therefore, the regulation of the «content» of sites on the Internet is difficult or causes undesirable consequences, since it is carried out on the basis of «machine» logic.

Keywords: Internet Regulation, machine thinking, man.

¹ О внесении изменений в Федеральный закон «О связи» и Федеральный закон «Об информации, информационных технологиях и о защите информации»: Федеральный закон от 01.05.2019 г. N 90-ФЗ. Режим доступа: <https://rg.ru/2019/05/07/fz90-dok.html> (дата обращения: 18.05.2019).

² Путин потребовал принять законы, которые не будут мешать цифровой экономике // CNews. Издание о высоких технологиях [Электронный ресурс]. Режим доступа: http://www.cnews.ru/news/top/2019-02-20_putin_prikazal_nastroit_zakonodatelstvo_na (дата обращения: 18.05.2019).

Чёрный Антон Васильевич
Студент Института юстиции
Уральский государственный юридический университет
(г. Екатеринбург)
Paktoha1206@gmail.com

ТЕХНОЛОГИИ ОХРАНЫ РЕЗУЛЬТАТОВ ИНТЕЛЛЕКТУАЛЬНОЙ ДЕЯТЕЛЬНОСТИ

Аннотация: В статье рассматриваются особенности интеллектуальной собственности, ее виды, а также технические средства для защиты результатов интеллектуальной деятельности на примере защиты авторских прав на звуки, музыкальные произведения, видеофайлы и фильмы. В статье описаны технические средства, которые использовались раньше, путь их развития, и как они выглядят сейчас. Также статья поднимает проблемы пренебрежения данными правами и последствий, вытекающих из этого.

Ключевые слова: интеллектуальная собственность, интеллектуальная деятельность, авторское право, нарушение авторских прав, защита авторских прав, технические средства для защиты результатов интеллектуальной деятельности, ТСЗАП.

В информационную эру, когда с каждым годом технический прогресс ускоряется, становясь все быстрее и быстрее, а от интеллектуальной деятельности и ее результатов зависят все сферы общественной жизни, трудно представить нашу жизнь без интеллектуальной собственности. Именно поэтому каждое государство нуждается в сохранении и развитии этого относительно молодого вида собственности. Для этих целей 26 июня 2000 года вступила в силу Всемирная Декларация по интеллектуальной собственности, в которой закреплено следующее определение понятия интеллектуальная собственность – «любая собственность, признаваемая по общему согласию в качестве интеллектуальной по характеру и заслуживающей охраны, включая, но не ограничиваясь научными и техническими изобретениями, литературными или художественными произведениями, товарными знаками и указателями деловых предприятий, промышленными образцами и географическими указаниями»¹.

Но как же появляется интеллектуальная собственность, и что такое интеллектуальная деятельность? Интеллектуальная деятельность – умственная, мыслительная, познавательная и творческая деятельность человека...»². Достаточно широкое определение, под которое можно уместить даже рисунок в тетрадке, который был нарисован на лекции. Конкретизировать данный термин нам поможет 1225 статья Гражданского кодекса, в которой закреплены охраняемые результаты интеллектуальной деятельности и средства индивидуализации, а именно:

- произведения науки, литературы и искусства;
- программы для электронных вычислительных машин (программы для ЭВМ);
- базы данных;
- исполнения;
- фонограммы;

¹ Всемирная декларация по интеллектуальной собственности от 26 июня 2000 г. // Интеллект. собственность. Авторское право и смежные права. № 4. 2002. С. 14.

² «Методические рекомендации по признанию результатов интеллектуальной деятельности единой технологией» (утв. Минобрнауки РФ 01.04.2010).

- сообщение в эфир или по кабелю радио- или телепередач (вещание организаций эфирного или кабельного вещания);
- изобретения;
- полезные модели;
- промышленные образцы;
- селекционные достижения;
- топологии интегральных микросхем;
- секреты производства (ноу-хау);
- фирменные наименования;
- товарные знаки и знаки обслуживания;
- наименования мест происхождения товаров;
- коммерческие обозначения.

Как можно заметить, получился внушительный список, в котором вопреки мнению обывателей не только музыка с фильмами, за которые все чаще приходится платить, но и необходимые для развития науки, промышленности, общества и каждого человека средства.

Все эти нематериальные и непохожие друг на друга блага нужно защищать. Для обеспечения надлежащего уровня защиты применяются различные способы в зависимости от их вида:

- результаты литературной и художественной деятельности, такие как книги, картины, фильм музыка, аудио или видеозаписи, а также программное обеспечение защищены авторским правом или смежными правами;
- технологические открытия, а также технологии охраняются патентным правом;
- средства индивидуализации такие как знаки обслуживания; символы и даже формы, звуки, запахи, цвета, которые позволяют отличать одни товары и услуги от других, могут охраняться с помощью товарных знаков;
- определённые особенности внешнего вида объектов, например, предметов мебели, элементов кузова автомобиля, столовых приборов или ювелирных изделий могут охраняться посредством института промышленных образцов;
- наименования мест происхождения товаров и коммерческая тайна также считаются разновидностями интеллектуальной собственности, и большая часть государств предоставляет таким объектам тот или иной объем правовой охраны;
- сорта растений преимущественно охраняются специальным правом на селекционные достижения, относящимся к области прав интеллектуальной собственности, но могут охраняться и традиционными патентами, либо двумя способами одновременно¹.

Хотелось бы подробно раскрыть техническую сторону защиты авторских прав, так как именно с ними мы сталкиваемся каждый день, но в то же время пренебрежение правами авторов является обыденностью, а многие люди даже не догадываются об его нарушении.

Авторское право защищает и тем самым стимулирует создание различных произведений искусства и творчества, помогая авторам монетизировать свой труд. Помимо простого признания авторства, охрана авторских прав включает в себя технические средства для защиты результатов интеллектуальной деятельности (ТСЗАП; англ. DRM – digital rights management). 1299 статья Гражданского кодекса раскрывает определение данных средств: «Техническими средствами защиты авторских прав признаются любые технологии, технические устройства или их компоненты, контролирующие доступ к произведению, предотвращающие либо ограничивающие осуществление действий, которые не разрешены автором или иным правообладателем в

¹ Рекомендации ICC по интеллектуальной собственности // Обзор актуальных вопросов для предпринимателей и органов власти / Международная торговая палата. 2017. № 13.

отношении произведения». Из этого определения можно сделать вывод, что данные технологии должны обеспечить контроль за распространением копий, а также защитить от неразрешенного доступа защищенные файлы.

Для разных видов объектов защиты используются разные технологии. Для правообладателей звуков и музыкальных произведений борьба началась с появлением аудио-CD, которые для нас уже ушли в прошлое, но во многих более развитых странах с другим уровнем защиты авторского права и более серьезным наказанием за его нарушение, диски до сих пор пользуются большим спросом.

Одной из первых технологий по их защите является созданное компанией Sony BMG Music Entertainment, Inc специальное программное обеспечение для прослушивания аудиофайлов, записанное на дисках их производства ограничивающее действия с аудиофайлами, помимо этого программа не позволяла записывать аудиопоток. Данная программа устанавливалась на компьютер и скрывалась руткитом, а также не могла быть удалена с компьютера¹. Но в то же время она имела в себе критические уязвимости, которые позволяли использовать ее троянским программам, из-за чего компания была вынуждена отозвать из магазинов миллионы дисков, а также выплатить компенсации пострадавшим. По этим причинам данный вид DRM защиты использовался только с 2005 года до января 2007 года, а все вышеперечисленные проблемы использования DRM на дисках послужили главной причиной отказа крупнейших лейблов от использования этой технологии².

Иной подход к DRM был выбран компаниями Apple и Microsoft, которые защищали аудиофайлы не на физических носителях, а при распространении в цифровом виде через интернет. Технология в этом случае заключалась в шифровании аудиофайлов в формате MP4 с помощью симметричного алгоритма блочного шифрования³ (англ. Advanced Encryption Standard), в котором ключ шифрования генерировался случайным образом на сервере компании и дополнительно шифровался ключом пользователя. В данном случае интересна политика компаний по использованию данной защиты, так как она кардинально отличается. DRM от Apple – FairPlay (англ. Честная игра) является примером правильного подхода к защите, так как позволяет прослушать купленный контент на 5 устройствах, а в дальнейшем сделать их сброс и прослушать на других, помимо этого путь в директорию к файлу открыт, что по сути открывает к нему полный доступ. Microsoft же в своей DRM защите разрешили доступ к аудио только с одного устройства, а также ограничили доступ к нему, из-за чего данная защита была взломана еще до выхода и провалилась в дальнейшем⁴.

Сейчас Apple в своем магазине контента iTunes не использует DRM защиту, так как схемы DRM у разных звукозаписывающих организаций отличаются и из-за этого могут не воспроизводиться на некоторых устройствах. Интересным примером такого отказа может послужить заявление немецкой компании по онлайн-продаже музыки Musicload, они заявляют, что причиной их отказа от DRM защиты стали обращения потребителей, среди которых примерно 75% всех жалоб в службу поддержки были от клиентов, которых не устраивала DRM защита.

¹ Russinovich M. Sony, Rootkits and Digital Rights Management Gone Too Far. 2005. Режим доступа: <https://blogs.technet.microsoft.com/markrussinovich/2005/10/31/sony-rootkits-and-digital-rights-management-gone-too-far/> (дата обращения 18.05.2019).

² Троян эксплуатирует «брешь» в ПО Sony DRM по защите от копирования // ДиалогНаука [Электронный ресурс]. Дата обновления: 11.11.2005. Режим доступа: http://www.dialognauka.ru/press-center/news/3697/?sphrase_id=48199 (дата обращения: 18.05.2019).

³ ГОСТ Р 54713-2011. Звуковое вещание цифровое. Кодирование сигналов звукового вещания с сокращением избыточности для передачи по цифровым каналам связи. MPEG-2, часть VII: усовершенствованное кодирование звука (MPEG-2 AAC). М.: Стандартинформ, 2013.

⁴ Защиту MICROSOFT DRM опять взломали // SecurityLab.ru [Электронный ресурс]. Дата обновления: 18.07.2007. Режим доступа: <https://www.securitylab.ru/news/299635.php>. (дата обращения: 18.05.2019).

В наше время самым актуальным способом защиты и монетизации аудиофайлов являются стриминговые сервисы, такие как Apple Music, Google Play Музыка, Яндекс.Музыка, Spotify, Deezer, Soundcloud, Boom (музыка Вконтакте) и другие. Данные вид распространения музыки является логическим продолжением технологий DRM защиты, применяемых ранее. У каждого из сервисов, перечисленных выше, есть свои плюсы и минусы, но работают они все по одному принципу: пользователь либо оплачивает доступ к музыкальной библиотеке в специальном приложении или в своем аккаунте через браузер, либо в нем же слушает музыку, но с ограничениями и рекламой. Данный подход является одним из самых успешных, так как устраивает и правообладателей и потребителей¹, именно поэтому в 2016 году 51% процент выручки всей музыкальной индустрии США приходился именно на стриминговые сервисы, а число их платных подписчиков превысило 100 миллионов².

Борьба с нелегальным распространением видеофайлов и фильмов началась в 1996 году, тогда производители DVD начали использовать технологию CSS (Content Scramble System), которая заключалась в шифровании информации на дисках и ее обязательной расшифровке DVD-проигрывателем перед воспроизведением. Таким образом, перед воспроизведением каждый проигрыватель производил сначала аутентификацию проигрывателя и DVD-диска, а затем дешифрование файлов³. Но данная технология не являлась устойчивой к взломам из-за короткого ключа шифрования, он был равен 40 битам, также ее поддержка была достаточно дорогой, так как все части DVD-проигрывателей, участвующих в алгоритмах CSS, а именно сами проигрыватели, DVD-диски, DVD-приводы и специальный хост подлежали обязательному лицензированию в DVD Copy Control Association (DVD CCA)⁴.

Поэтому в апреле 2005 года была представлена новая улучшенная система – AACS (Advanced Access Content System; с англ. – «улучшенная система доступа к содержимому»). Данная технология была разработана при участии таких крупных компаний, как Microsoft, Panasonic, Warner Bros., Disney, Intel, IBM, Sony и других. В улучшенной системе был усложнен порядок шифрования, в отличие от CSS, где все проигрыватели одной модели были оснащены одним ключом шифрования, в AACS каждый проигрыватель имел свой собственный ключ расшифрования, что позволяло точно блокировать ключи, которые были взломаны, из-за чего дальнейшее дешифрование материалов в обход защиты становилось невозможным. Но и эта технология была взломана, так как вне зависимости от количества уровней шифрования, ключи находятся в оперативной памяти компьютера, что позволяет создать их виртуальную копию и с ее помощью обойти аутентификацию. Именно поэтому, спустя год после выхода AACS большая часть ключей, а также иные средства обхода данного вида защиты каждый желающий мог найти в интернете.

Еще одним средством DRM является региональная защита дисков. Данная технология состоит в нанесении специальной маркировки на дисках в зависимости от региона их распространения. Помимо усложнения копирования данная технология используется для запрета доступа к контенту в государствах, где он еще официально не вышел и для установления различных цен в зависимости от региона. Дифференциация цен на один товар и закрепление их за определенными регионами противоречит положениям фритредерства⁵ (англ. free trade – «свободная торговля») провозглашающим свободу

¹ Птушко А.С. Аудиостриминг как новый вид музыкального интернет-вещания (на примере стриминг-сервиса soundcloud) // Медиасреда. 2017. С. 232-235.

² Roettgers J. Streaming Services Generated More Than 50% of All U.S. Music Industry Revenue in 2016 // Variety.com [Электронный ресурс]. Режим доступа: <https://variety.com/2017/digital/news/streaming-services-us-music-revenue-2016-1202019504/> (дата обращения: 18.05.2019).

³ Taylor J. DVD Demystified. McGraw-Hill, 2006. 700 p.

⁴ Kesden G. Operating Systems: Design and Implementation.

⁵ Холопов А. В. История экономических учений. М.: Эксмо, 2009.

торговали, невмешательство в частнопредпринимательскую сферу жизни общества¹ из-за чего, данная технология не применяется в некоторых странах, например в Австралии².

Как уже говорилось ранее, обход технических средств защиты авторских прав и пренебрежение этими правами давно стали нормой, особенно в нашей стране, и это является огромной проблемой как для авторов, так и для потребителей, ведь без должной защиты и поддержки не будет никакого развития, первые не получают средств, а вторые не получают продукта. Может быть именно поэтому самые крупные ИТ-компании, гиганты игровой, музыкальной и кинематографической индустрии преимущественно базируются именно в тех странах, где результаты их интеллектуальной деятельности подлежат надёжной защите? Помимо этого, любое пиратство искажает здоровую конкуренцию в условиях рынка, ведь невозможно конкурировать с теми, кто бесплатно пользуется чужим трудом и при этом не расходует средства на исследования, разработку, рекламирование своего продукта. Поэтому технические средства для защиты результатов интеллектуальной деятельности должны развиваться, а интеллектуальная собственность должна защищаться не меньше материальной.

Список литературы

1. Russinovich M. Sony, Rootkits and Digital Rights Management Gone Too Far. 2005. Режим доступа: <https://blogs.technet.microsoft.com/markrussinovich/2005/10/31/sony-rootkits-and-digital-rights-management-gone-too-far/>.
2. Птушко А.С. Аудиостриминг как новый вид музыкального интернет-вещания (на примере стриминг-сервиса soundcloud) // Медиасреда. 2017. С. 232-235.
3. Taylor J. DVD Demystified. McGraw-Hill, 2006. 700 p
4. Kesden G. Operating Systems: Design and Implementation.
5. Холопов А. В. История экономических учений. М.: Эксмо, 2009.
6. Блауг М. Система Рикардо // Экономическая мысль в ретроспективе = Economic Theory in Retrospect. М.: Дело, 1994. С. 82–135.
7. Consumers in dark about DVD imports / Australian Competition and Consumer Commission. Режим доступа: <https://www.accc.gov.au/media-release/consumers-in-dark-about-dvd-imports-accc>.

Anton V. Cherny

Student of Institute of Justice
Ural State Law University
(Russia, Yekaterinburg)
Paktoha1206@gmail.com

TECHNOLOGIES OF PROTECTION OF RESULTS OF INTELLECTUAL ACTIVITY

Abstract: the article discusses the features of intellectual property, its types, as well as technical means to protect the results of intellectual activity on the example of copyright protection for sounds, music, video files and movies. The article describes the technical means that were used before, the way of their development, and how they look now. The article also raises the problem of neglect of these rights and the consequences arising from this.

Keywords: intellectual property, intellectual activity, copyright, copyright infringement, copyright protection, digital rights management, DRM.

¹ Блауг М. Система Рикардо // Экономическая мысль в ретроспективе = Economic Theory in Retrospect. – М.: Дело, 1994. – С. 82–135.

² Consumers in dark about DVD imports. Australian Competition and Consumer Commission (21 декабря 2000 г.).

Чуваткин Борис Юрьевич
Студент Института юстиции
Уральский государственный юридический университет
(г. Екатеринбург)
ch-boris97@mail.ru

РЕЗУЛЬТАТ РАБОТЫ ИСКУССТВЕННОЙ НЕЙРОННОЙ СЕТИ КАК ОБЪЕКТ ИНТЕЛЛЕКТУАЛЬНЫХ ПРАВ*

Аннотация: В работе раскрывается понятие «нейронная сеть» и определяются проблемы правовой защиты результатов работы нейронных сетей в Российской Федерации.

Ключевые слова: искусственная нейронная сеть, интеллектуальная система, интеллектуальная собственность, интеллектуальная деятельность, творческая деятельность, искусственный интеллект, результат работы искусственной нейронной сети.

Информационные технологии стали незаменимыми в жизни каждого современного человека. Использование информационно-телекоммуникационных сетей, баз данных, компьютерных устройств, развитие телекоммуникационной инфраструктуры путём информатизации общества и государственных органов, всё это накладывает отпечаток на жизнь каждого человека. Право всегда догоняет реальную жизнь и общественные отношения. Это происходило раньше, в Римской Империи первоначально переход права собственности от одного лица к другому осуществлялся по средству манципации (лат. Mancipatio), но путём развития общественных отношений в Римской Империи появился другой способ перенесения права собственности – традиция (лат. Traditio), воспринятый от права народов (лат. Jus gentium), благодаря своему удобству так как для того чтобы передать право собственности была необходима лишь фактическая передача вещи, в то время как в манципации требовалось привлечение 5 свидетелей и весовщика¹. Другой пример – это развитие норм трудового права. Как пример США в которых во второй половине 19 начале 20 века были закреплены нормы, ограничивающие женский и детский труд², из-за борьбы пролетариата с тяжёлыми условиями труда. Это происходит и сегодня, путём включения норм касающихся информатизации и развития информационных технологий, как пример ст. 164.1 УПК РФ³, регулирующая изъятие электронных носителей информации или ст. 278.1 УПК РФ, регулирующая допрос свидетеля с использованием систем видеоконференц-связи, или введение законов связанных с информационными технологиями, как пример федеральный закон «Об информации, информационных технологиях и о защите информации»⁴. Но в данной работе речь пойдёт о правовом регулировании вопросов связанных с искусственными нейронными сетями.

* Исследование выполнено при финансовой поддержке Российского фонда фундаментальных исследований в рамках научного проекта 18-29-16001\18 «Комплексное исследование правовых, криминалистических и этических аспектов, связанных с разработкой и функционированием систем искусственного интеллекта».

¹ Римское частное право. Учебник / под ред. И. Б. Новицкого, И. С. Перетерского. М.: Изд. «Зерцало-М», 2012.

² Развитие трудового законодательства США в XIX-XX вв. [Электронный ресурс]. Режим доступа: <https://studentu.info/gosudarstvo-i-pravo/vseobshchaya-istoriya-gosudarstva-i-prava/razvitie-trudovogo-zakonodatelstva-ssha-v-xix-xx-vv> (дата обращения 18.05.2019).

³ Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 г. N 174-ФЗ (ред. от 01.04.2019, с изм. от 17.04.2019) (с изм. и доп., вступ. в силу с 12.04.2019) // Российская газета. 22.12.2001. N 249.

⁴ Об информации, информационных технологиях и о защите информации: Федеральный закон от 27.07.2006 г. N 149-ФЗ // Российская газета. 29.07.2006. N 165.

Оксфорд Школа Мартина ещё в 2013 году говорила, что 47 % рабочих мест будет автоматизировано в течении ближайших 20 лет¹. Главную роль в данной работе отводилась интеллектуальным системам, способным обучаться и выполнять однотипную работу за человека. В связи с развитием и разработкой интеллектуальных систем существовало большое количество концепции, одной из концепции 80-х годов 20 века был парадокс Моравека, который заключался в том, что высококогнитивные процессы требуют относительно небольшого количества вычислений, в то время как на низкоуровневые сенсомоторные операции требуют большего количества вычислительной мощности. В современности данный парадокс раскрывается тем, что информационную систему легче научить сложным действиям взрослого человека, как например игра в шахматы, чем научить интеллектуальную систему деятельности доступной годовалому ребёнку по восприятию и мобильности, как пример распознавание предметов по их изображению. Этой концепцией подтверждался тезис о том, что интеллектуальную систему сложно научить творческой деятельности. В науке данная концепция нашла отражение в области машинного обучения, изучающего компьютерные алгоритмы способные обучаться самостоятельно, для решения проблемы сложности обучения информационных систем низкоуровневые операциям, связанным с восприятием. Разбираясь с понятиями данной науки стоит сказать, что нейронная сеть определяется как математическая модель, её аппаратное или программное построение, по принципу функционирования и организации нейронных сетей нервных клеток живого организма. Стоит заметить, что нейронная сеть лишь один из способов реализации искусственного интеллекта. В то же самое время искусственный интеллект – это свойство нейронной сети и иной интеллектуальной системы выполнять творческую деятельность, которую как считают многие может выполнять лишь человек.

Искусственная нейронная сеть способна к осуществлению творческой деятельности путём обучения. До 2010 года считалось, что обучать нейронную сеть бессмысленно из-за ошибок, которые допускала нейронная сеть, это было связано с тем, что не имелось достаточной базы изображений и данных для обучения нейронной сети и не было эффективных методов обучения нейронной сети, так как обучались только последние слои нейросети. Данная проблемы были решены созданием базы изображений ImageNet, содержащих огромное количество изображений и развития сети «интернет», с помощью которых система могла получить необходимые знания и развития 3 систем обучения искусственной нейронной сети: Джеффри Хинтона придумавшего обучение каждого слоя сети с помощью машины Больцмана, Яна Лекуна использующего сверточную нейронную сеть для распознавания изображений и Иосуа Бенджио создавшего каскадный автокодировщик задействующий все слои глубокой нейросети. Именно с этим связана современная популярность нейросетей и их обучение.

В результате обучения нейронная сеть начинает самостоятельно создавать различные продукты творческой деятельности. Учёные из лаборатории X Labs транснациональной публичной корпорации «Google» создали нейронную сеть и предоставили ей большое количество различных изображений. Обучаясь самостоятельно нейронная сеть сформировала для себя концепцию «Кошки» и научилась распознавать кошек. Нейронная сеть X Labs в дальнейшем смогла смоделировать изображение кошки², получив тем самым объект авторского права произведение графики. Другой нейронной системой, обладающей свойством искусственного интеллекта является нейросеть «Яндекс», способная анализировать музыкальные файлы и на основании них придумывать

¹ Frey C. B., Michael A. O. The future of employment: how susceptible are jobs to computerisation? [Электронный ресурс]. Режим доступа: https://www.oxfordmartin.ox.ac.uk/downloads/academic/The_Future_of_Employment.pdf (дата обращения 18.05.2019)

² Самообучающаяся компьютерная сеть // МирТесен [Электронный ресурс]. Режим доступа: <https://mt-smi.ru/blog/43723013708/Samoobuchayuschayasya-kompyuternaya-set?nr=1> (дата обращения 18.05.2019)

и записывать текст и музыку в песни. Нейросетью «Яндекс» уже был издан музыкальный альбом «Нейронная сеть»¹. Есть множество и других примеров.

Возможно ли защитить результат данной работы искусственной нейронной сети или интеллектуальной системы? Именно такой вопрос зададут ряд компаний и корпорации, вкладывающих свои силы в развитие нейронных сетей и интеллектуальных систем, когда узнают, что результатами работы их систем без разрешения и приобретения начнёт пользоваться широкий круг лиц. Под интеллектуальной собственностью в Российской Федерации согласно п.32 Постановления Пленума Верховного Суда Российской Федерации № 10² понимаются результаты интеллектуальной деятельности и приравненные к ним средства индивидуализации, но не права возникающие на результаты интеллектуальной деятельности и приравненные к ним средства индивидуализации. Является ли результат работы искусственной нейронной сети интеллектуальной деятельностью?

В Российской Федерации результаты работы искусственной нейронной сети или интеллектуальной системы не является интеллектуальной собственностью, а, следовательно, и объектом интеллектуальной деятельности или приравненных к ним средств индивидуализации. Это исходит из ряда причин. Если разобраться с самим понятием интеллектуальной деятельности, то под результатами интеллектуальной деятельности понимается закрытый перечень продуктов творческого труда и приравненных к ним других нематериальных объектов, на которые у их правообладателей возникают интеллектуальные права. Закрытый перечень указан в ст. 1259 Гражданского Кодекса РФ, в которой перечислены объекты авторских прав. Из определения можно выделить два критерия, для выделения интеллектуальной деятельности: первый критерий это творческая деятельность, второй критерий результат данного труда должен иметь объективное выражение³. Под творческой деятельностью согласно ст. 3 ФЗ «Основ законодательства Российской Федерации о культуре»⁴ понимается создание культурных ценностей и их интерпретация. На основании ст. 1228 ГК РФ выполнять творческую деятельность может только человек. Это обозначает, что искусственная нейронная сеть создавая какой-либо объект, не создаёт объект авторских прав, так как она не создаёт её творческим трудом. Некоторые авторы высказывают точку зрения, что под творческой деятельностью в интеллектуальном праве понимается – самостоятельная свободная интеллектуальная деятельность, выходящая за пределы обычной технической работы⁵. Но не то ни другое определение не позволяет признать, что интеллектуальная система, создавая результат своей работы получает его творческим путём. Вторым критерий - это объективное выражение во вне, которое подразумевает под собой форму выражения результата творческой деятельности: устную, письменную, объёмно-пространственную, хореографическую и многие другие. В данном случае искусственная нейронная сеть создаёт объект в форме выражения: устно, графической или иным образом. Критерии необходимые для признания объекта, полученного при работе интеллектуальной системы объектом авторских прав, не совпадают полностью. Чем же тогда является результат работы нейронной сети?

Неидентичным являются понятия деятельность по использованию программного обеспечения с целью создания объекта авторских прав человеком и использование

¹ Нейросеть, разработанная сотрудниками Яндекса, написала тексты в стиле Егора Летова [Электронный ресурс]. Режим доступа: <https://apparat.cc/news/neurodefence/> (дата обращения 18.05.2019).

² О применении части четвертой Гражданского кодекса Российской Федерации: постановление Пленума Верховного Суда РФ от 23.04.2019 N 10 // Российская газета. 06.05.2019. N 96.

³ Гонгало Б. М. Учебник гражданское право. Том 1. М.: Изд. Статут, 2017.

⁴ Основы законодательства Российской Федерации о культуре (утв. ВС РФ 09.10.1992 N 3612-1) (ред. от 05.12.2017) // Российская газета. 17.11.1992. N 248.

⁵ Признаки творчества в авторском праве [Электронный ресурс]. Режим доступа: <https://sumip.ru/biblioteka/avtorskoye-pravo/teoreticheskie-aspekty-istoriya-avtorskogo-prava/priznak-tvorchestva-v-avtorskom-prave/> (дата обращения 18.05.2019)

искусственной нейронной сети для создания объекта авторских прав. В первом случае человек использует программное обеспечение лишь как инструмент для создания объекта на который будут распространяться авторские права и становится автором данного объекта по факту того что он осуществил творческую деятельность и у результата работы есть форма выражения. Как пример использование текстового редактора для написания научной статьи. Во втором случае при использовании нейронной сети, когда человек вводит команду нейронной сети создать изображение или написать текст у человека не может возникнуть никаких прав на данный объект, так как творческой деятельностью человек не занимался, хоть у получившегося объекта и есть форма выражения. В настоящее время данный объект не будет результатом интеллектуальной деятельности, следовательно, он не будет подлежать защите, что является неправильным.

Можно сказать, что права на данное произведение получит автор создавший нейронную сеть, но это тоже будет неправильно, согласно действующему законодательству. Если использовать такую логику, то получится, что дед приобретает авторские права от отца, а тот приобретает авторские права от сына осуществившего интеллектуальную деятельность для создания объекта авторского права. Программисты создавшие интеллектуальную систему не прилагают никакой творческой деятельности при работе интеллектуальной системы или искусственной нейронной сети. Результат такой работы не является выполненным в соавторстве, так как согласно ст. 1258 ГК РФ произведение должно быть создано совместным творческим трудом. Но искусственная нейронная сеть не может осуществлять творческую деятельность, а создатели нейронной сети не прикладывали никаких сил для производства продукта полученного искусственной нейронной сетью. Дополнительно для соавторства нет такого условия, как согласие соавторов на совместное создание произведения, так как искусственная нейронная сеть не может дать согласия, так как она не обладает правосубъектностью, а создатель программист и иной субъект не может предложить данной сети сделать произведение в соавторстве.

Искусственная нейронная сеть или интеллектуальная система, как было сказано ранее, не является субъектом права, так же, как и животные хотя они могут создавать своим трудом объекты, указанные в ст. 1259 ГК РФ. Деятельность искусственного интеллекта, так же как животного не признаётся творческой. Если животное производит действия по созданию объектов авторских прав бессознательно (случайно), то нейронная сеть выполняет данную деятельность целенаправленно, творчески. Если мы будем говорить про объекты авторского права созданные животными, то можно вспомнить историю макаки в Индонезии, сделавшую знаменитые снимки из-за которых проходил спор фотографа за наделение его авторскими правами на данные снимки. Федеральный арбитражный суд США 12 июня 2017 года подтвердил позицию, что автора у данных снимков нет, а следовательно ни у кого не возникло авторских прав¹. Мы не можем применять практику иностранных государств при решении вопросов в Российской Федерации, потому что регулирование интеллектуального права во всех странах проходит по-разному. Однако такая практика указывает, что могут существовать объекты, указанные в ст. 1259 ГК РФ, не имеющие автора и не подлежащие защите, являющиеся по сути всемирным достоянием. Тем самым подтверждается, что по действующему законодательству искусственная нейронная сеть не может быть правообладателем авторских прав на созданный ей объект.

Имеет ли данная проблема решения сегодня? Многие назовут данную проблему научной, не имеющей отношения к действительности, но решать её с дальнейшим быстрым развитием компьютерной техники придётся достаточно скоро. В настоящее

¹ Фотограф разорился, судясь с обезьяной за авторское право на её снимок [Электронный ресурс]. Режим доступа: <https://yandex.ru/turbo?text=https%3A%2F%2Fcameralabs.org%2F11613-fotograf-razorilsya-sudyas-s-obezyanoj-za-avtorskoe-pravo-na-ejo-snimok&d=1> (дата обращения 18.05.2019)

время мы не признаем за искусственной нейронной сетью правосубъектность. Стоит заметить, что, создавая интеллектуальную систему, человек старается воссоздать свой образ мышления создавая прообраз нейронной сети. Нейронная сеть так же анализирует информацию путём получения опыта и на основании этого формирует свои действия, у неё так же как у человека при изучении ситуации возникают метапонятия (интерпретация понятий и опыта полученных на прошлых стадиях). Возможно стоит признать правосубъектность за интеллектуальными системами, а значит наличие у них возможности на получение интеллектуальных прав и признать, что интеллектуальные системы осуществляют интеллектуальную деятельность, однако законным представителем интеллектуальных систем назначить человек или организация создавшая данную систему. Часто ради справедливости и пользы требуется соблюдение юридических правил, данная конструкция будет правовой фикцией. Фактически создатель интеллектуальной системы будет получать прибыль с объекта интеллектуальных прав, полученного от работы нейронной сети или интеллектуальной системы, и будет иметь возможность защищать право на такой произведённый объект.

Интеллектуальное право самый современный быстроразвивающийся раздел гражданского права. Включение в гражданский кодекс норм защищающих результаты работы искусственных нейронных сетей, обладающих свойством искусственного интеллекта — это лишь вопрос времени. Как и когда произойдёт включение данных норм в данный момент определить практически невозможно, но возможно предложить конкретное решение возможных проблем. С развитием современного общества появляется множество новых нестандартных проблем, которые следует решать. Каждое поколение стоит перед порогом открытий и развития чего-то нового. Мы не должны останавливаться на достигнутом, задача юриста воспринять современную действительность и урегулировать её в норме права, для дальнейшего справедливого применения.

Список литературы

1. Frey C. B., Michael A. O. The future of employment: how susceptible are jobs to computerisation? [Электронный ресурс]. Режим доступа: https://www.oxfordmartin.ox.ac.uk/downloads/academic/The_Future_of_Employment.pdf
2. Гонгало Б. М. Учебник гражданское право. Том 1. М.: Изд. Статут, 2017. 511 с.
3. Признаки творчества в авторском праве [Электронный ресурс]. Режим доступа: <https://sumip.ru/biblioteka/avtorskoye-pravo/teoreticheskie-aspekty-istoriya-avtorskogo-prava/priznak-tvorchestva-v-avtorskom-prave/>
4. Развитие трудового законодательства США в XIX-XX вв. [Электронный ресурс]. Режим доступа: <https://studentu.info/gosudarstvo-i-pravo/vseobshchaya-istoriya-gosudarstva-i-prava/razvitie-trudovogo-zakonodatelstva-ssha-v-xix-xx-vv>.
5. Римское частное право. Учебник / под ред. И. Б. Новицкого, И. С. Перетерского. М.: Изд. «Зерцало-М», 2012. 560 с.

Boris Y. Chuvatkin

Student of Institute of Justice
Ural State Law University
(Russia, Yekaterinburg)
ch-boris97@mail.ru

RESULT OF WORK OF THE ARTIFICIAL NEURAL NETWORK AS OBJECT OF THE INTELLECTUAL RIGHTS

Annotation: In this paper the concept a neural network is revealed and problems of legal protection of results of work of neural networks in the Russian Federation are defined.

Keywords: artificial neural network, intellectual system, intellectual property, intellectual activity, creative activity, artificial intelligence, result of work of a neural network.

Щелконогова Елена Владимировна

Кандидат юридических наук, доцент кафедры уголовного права
Уральский государственный юридический университет
(г. Екатеринбург)
Shelkonogova-ele@mail.ru

УГОЛОВНОЕ ПРАВО ON-LINE: ТЕОРИЯ И ПРАКТИКА ЦИФРОВИЗАЦИИ

Аннотация: Актуальность темы исследования обусловлена активным входом в повседневную жизнь человека цифровых и компьютерных технологий. Одной из сфер жизнедеятельности, в которых компьютеризация активно набирает обороты является юриспруденция. Достаточно упомянуть о существовании различных справочно-правовых баз правовых актов, оснащенных возможностью поиска по различным параметрам.

Несмотря на то, что тема цифровизации активно разрабатывается в юридической литературе, статья обладает новизной, т.к. раскрывает различные сферы, в которых может быть полезно использование компьютерных программ, содержащих алгоритмы, т.е. последовательность определенных действий. Также рассматривается проблема соблюдения принципа справедливости при принятии решений, имеющих юридически важное значение компьютером или квалифицированным юристом. Помимо изложенного проблема цифровизации юриспруденции рассматривается, как с точки зрения проникновения того, что компьютерные алгоритмы действий могут помогать юристу в работе, так и с позиции того, что право, в частности уголовное право, призвано защищать сферу компьютерной деятельности.

Ключевые слова: искусственный интеллект, алгоритм квалификации, принцип справедливости, компьютерная преступность.

«Кто владеет информацией, тот владеет миром».
У. Черчилль

Искусственный интеллект все более плотно входит в различные сферы нашей жизни, не обходя стороной и юридическую сферу. Достаточно упомянуть о проблемах, связанных с криптовалютами и интеллектуальной деятельностью. Однако думается, что соотношение понятий искусственного разума и юридической науки можно рассмотреть с одной стороны в том аспекте, что цифровизация активно применяется в какой-то иной сфере деятельности, а юриспруденция регулирует эту сферу и поэтому вынуждена учитывать особенности цифрового влияния на какие-либо события, правоотношения и т.д. (например, охрана прав на результаты интеллектуальной деятельности в сети Интернет, авторство компьютерных программ, авторство музыки и фильмов, используемых без согласия автора).

С другой стороны, цифровизация возможна и в самой юриспруденции, т.е. создание интернет-баз данных законов, построение компьютерных алгоритмов, в которых пошагово прописываются действия юриста в конкретной ситуации. Кстати, алгоритмизация деятельности не столь и новый прием, поскольку он использовался и ранее в различных сферах жизнедеятельности, например, в производствах, связанных с точными науками: алгоритм лечения болезни, алгоритм обучения человека новым знаниям и пр. Однако если ранее, до массового появления компьютеров и программ, эти алгоритмы прописывались на бумажных носителях или держались просто в голове человека (например, когда мастер передавал подмастерью опыт), теперь появилась возможность построения алгоритмов с помощью компьютерных программ.

Поскольку область юриспруденции чрезвычайно широка, так как призвана регулировать практически все сферы жизни, мы остановимся на такой отрасли, как уголовное право. И несмотря на то, что другие отрасли имеют свою специфику и интерес исследования проблематики использования цифровых приемов в этих отраслях также чрезвычайно высок, нам хотелось бы осветить именно сферу уголовного права в контексте исследуемого вопроса, хотя бы потому, что уголовное право связано с такими неотъемлемыми правами человека как право на жизнь, свободу.

Массовый интерес к проблеме цифровизации знания и различных мыслительных процессов способствует тому, что нередко высказываются опасения относительно того, что автомат (компьютер) может причинить что-либо негативное человеку своими действиями, аргументируется это в таком ключе, что автомат неодушевлен и зависит от различных технических особенностей, поэтому доверять ему нельзя. Хотя с другой стороны действия человека могут быть обусловлены субъективным отношением. Эта проблематика на самом деле имеет много общего с принципом справедливости, о котором писали также много, но в данном случае он приобретает важное значение при интерпретации в новом ключе.

Начиная с Аристотеля, принято выделять два вида справедливости: Уравнительная — относится к отношениям равноправных людей по поводу предметов («равным — за равное»). Она относится не непосредственно к людям, а к их действиям, и требует равенства (эквивалентности) труда и оплаты, ценности вещи и её цены, вреда и его возмещения. Распределительная — требует пропорциональности в отношении к людям согласно тому или иному критерию («равное — равным, неравное — неравным», «каждому своё»). Уравнительная справедливость является специфическим принципом частного права, тогда как распределительная — принципом публичного права, являющегося совокупностью правил государства как организации¹.

Если исходить из того, что уголовное право — это публичная отрасль, то в данном случае следует говорить о распределительной справедливости. Причем как отмечают теоретики данного принципа, отношения распределительной справедливости требуют участия по меньшей мере, трех людей, каждый из которых действует для достижения одной цели в рамках организованного сообщества. Один из этих людей, распределяющим, является «арбитром». Проецируя данные положения на ранее изложенное приходим к выводу, что в решении того или иного спора в любом случае необходим арбитр или судья. Однако, если мы все более внедряем цифровизацию в данном случае в процесс решения спора, то получается, что роль арбитра будет выполнять машина, а не человек. Безусловно, это радикальный подход, который возможно и затруднительно себе представить. Поэтому рассматривается и такой вариант, что компьютер будет лишь вспомогательным элементом для человека. Хотя с другой стороны такая функция уже давно используется, при применении тех же справочно-правовых баз, например. В таком случае, почему же вопрос о примени искусственного интеллекта с каждым днем набирает свою актуальность и звучит все более остро.

Возможно и потому, что, если какой-либо процесс не угасает, он может существовать стабильно или развиваться. Поэтому многие ученые, смотря в перспективу, ставят вопросы о дальнейшем сосуществовании человеческого усмотрения и роли механизма при принятии решений. Также необходимо подчеркнуть ту существенную разницу, которая имеется между областью точных наук и использованием компьютера, например, в производственном процессе и сферой гуманитарного знания, сферой обстоятельств человеческой жизни, которые являются индивидуальными. Такой вопрос, но, возможно в другом ракурсе, разработан философами права, которые постулируют о

¹ Справедливость // Википедия – свободная энциклопедия [Электронный ресурс]. Режим доступа: <https://ru.wikipedia.org/wiki/Справедливость> (дата обращения: 18.05.2019). См., например: Кашников Б. Н. Концепция общей справедливости Аристотеля: Опыт реконструкции // Этическая мысль. 2001. Вып. 2. С. 89-117.

том, что области естественных наук и гуманитарного знания необходимо разграничивать хотя бы потому, что верификация или проверка знания на подлинность в естественной сфере происходит при помощи опыта. Условия, в которых он проводится, можно повторять множество раз. В сфере же гуманитарного знания даже одно повторение тех же условий невозможно. Даже два совершенно одинаковых преступления будут отличаться друг от друга хотя бы временем совершения. То есть опытным путем проверить гуманитарные знания невозможно. Возникает вопрос: подходит ли такая логическая посылка компьютеру.

Необходимо отметить и то, что пока, как в сфере точных наук, так и гуманитарных, управление механизмами осуществляет все-таки человек. Думается, что рассмотрение проблематики использования искусственного интеллекта в сфере юриспруденции актуально и в том ракурсе, что и цифровая сфера также нуждается в правовом регулировании и уголовно-правовой охране. В частности, в УК РФ действует глава о компьютерных преступлениях, которая содержит такие составы, как неправомерный доступ к компьютерной информации, создание и использование вредоносных программ, неправомерное воздействие на информационную структуру РФ. Важно отметить, что данные составы с квалифицирующими признаками законодатель признает настолько общественно опасными, что относит к категории тяжких.

В структуру компьютерной преступности в Российской Федерации входят не только преступления в сфере компьютерной информации, но и большое количество преступных деяний, совершенных с помощью информационно-телекоммуникационных сетей¹. Компьютерная преступность (преступление с использованием *компьютера*) представляет собой любое незаконное, неэтичное или неразрешенное поведение, затрагивающее автоматизированную обработку *данных* или передачу данных. При этом, компьютерная информация является предметом или средством совершения *преступления*. Структура и динамика компьютерной преступности в разных странах существенно отличается друг от друга².

Если говорить об алгоритме квалификации преступлений, т.е. поиске нужной статьи при помощи компьютера, то такие исследования проводились. Например, в 1996 г. в МГУ была создана компьютерная программа оценки преступлений, совершенных с использованием оружия, а также при необходимой обороне. Думается, что разработка таких программ перспективна и была бы полезна. В свете соблюдения принципа справедливости важно отметить, что при разработке таких программ важна методика оценки и учета тех или иных обстоятельств. Эту методику необходимо заложить с учетом жизненных обстоятельств, но действия программы должны быть автоматизированы.

Алгоритм квалификации преступлений может быть построен по принципу движения от общего к частному путем ответов на вопросы, которые будут отсекают лишние по содержанию понятия. Такой алгоритм возможно построить как по отдельным главам Особенной части УК РФ, так и с учетом положений Общей части.

Рассмотрев некоторые аспекты возможного применения цифровизации в юриспруденции, важно отметить, что сама по себе компьютеризация оценивается представителями различных сфер либо как негативное явление, либо приветствуется. Например, доктор биологических наук, заведующая кафедрой проблем конвергенции естественных и гуманитарных наук Санкт-Петербургского гос. университета Т.В. Черниговская, участвуя в Гайдаровском форуме в 2018 году утверждала, что «прежде чем решать вопрос контроля над искусственным интеллектом, нужно задать себе вопрос: а есть ли у нас сейчас контроль над естественным интеллектом? Мы кардинально зависимы

¹ Евдокимов К. Н. Структура и состояние компьютерной преступности в РФ // Юридическая наука и правоохранительная практика. 2016. 1 (35). С. 86-94. Режим доступа: <https://cyberleninka.ru/article/n/struktura-i-sostoyanie-kompyuternoy-prestupnosti-v-rossiyskoy-federatsii> (дата обращения: 18.05.2019).

² Компьютерная преступность // Википедия – свободная энциклопедия [Электронный ресурс]. Режим доступа: https://ru.wikipedia.org/wiki/Компьютерная_преступность (дата обращения 18.05.2019).

от нашего мозга». «Уже сейчас появляется термин «Праздная цивилизация»¹. То есть ученый высказывает опасения о неконтролируемом процессе развития цифровых технологий, отсутствии контроля со стороны человека, развитие зависимостей.

Думается, что компьютеризация могла бы заменить человека в тех сферах, в том числе и юриспруденции, где не требуется творческий подход человека. В то же время у человека как раз освобождалось бы время для искусства, личностного роста. Однако если развитие компьютера достигнет такого уровня, что он сможет заменить и творческие способности человека, то такое развитие повлечет очень сильное изменение действительности. Возможно, человек столкнется с такой реальностью, которую не в полной мере сможет контролировать. С другой стороны, представить без компьютера сейчас практически все сферы деятельности, медицину, транспорт и др. невозможно. Все-таки необходимо определиться с тем, что цифровизация нашей жизни – это развитие человека, а не шаг назад. Проблематика, на наш взгляд, состоит в том, что теряется индивидуальный подход к жизненной ситуации. Компьютер не имеет чувственного и духовного опыта, поэтому с одной стороны можно назвать его беспристрастным, а с другой – отсутствие чувств влечет невозможность оценивать те или иные события как человек. Например, при совершении преступления определить, является ли это действие преступлением, т.е. общественно опасно оно или нет, а, возможно, это административное правонарушение – компьютер не сможет.

Наверное, юриспруденция на все сто процентов никогда не будет компьютеризирована, т.к. ответ на вопросы о добре и зле, степени причиненного вреда или нарушенных прав очень сложно (или невозможно) алгоритмизировать. Компьютер может стать (и уже является) вспомогательным элементом в вопросе, например, квалификации преступления. Контраргументом здесь может служить то, что человеческое усмотрение может быть предвзятым и субъективным. Конечно, если речь идет о преступном субъективизме, то такие действия уже будут относиться не сфере правоприменения, а к преступлению. Имеется в виду то, что как раз и необходимо, чтобы события действительности проходили через духовные принципы человека, квалифицированного специалиста. Достаточно упомянуть, что несмотря на бурный рост цифровизации суды присяжных действуют во всех субъектах РФ, а также и в зарубежном правосудии. То есть исследование фактов и их оценка человеком по-прежнему считаются правомочным способом признания того или иного деяния, например, преступным.

Таким образом, развитие цифровизации различных сфер жизнедеятельности человека, в том числе и юриспруденции происходит все более активно. Юриспруденция и отрасль уголовного права с одной стороны также воспринимают внедрения в их сферу компьютерных технологий, с другой стороны призваны регулировать и ставить под охрану законные правоотношения в этой области, такие как интеллектуальные права в Интернете, киберпреступность и др. цифровизация вызывает опасения у многих ученых в связи с тем, что компьютер в конечном счете заменит человека. Думается, что творческую деятельность человека и процесс оценки жизненных обстоятельств компьютер не сможет заменить. В то же время у человека появится больше возможностей для различной творческой деятельности.

Список литературы

1. Евдокимов К. Н. Структура и состояние компьютерной преступности в РФ // Юридическая наука и правоохранительная практика. 2016. 1 (35). С. 86-94. Режим

¹ Черниговская Т. Есть ли место человеку в будущем мире искусственного интеллекта [Электронный ресурс]. Режим доступа: http://json.tv/ict_video_watch/tatyana-chernigovskaya-spbgu-est-li-mesto-cheloveku-v-buduschem-mire-iskusstvennogo-intellekta-20180209120328 (дата обращения 18.05.2019).

доступа: <https://cyberleninka.ru/article/n/struktura-i-sostoyanie-kompyuternoy-prestupnosti-v-rossiyskoy-federatsii>.

2. Компьютерная преступность // Википедия – свободная энциклопедия [Электронный ресурс]. Режим доступа: https://ru.wikipedia.org/wiki/Компьютерная_преступность.

3. Справедливость // Википедия – свободная энциклопедия [Электронный ресурс]. Режим доступа: <https://ru.wikipedia.org/wiki/Справедливость>.

4. Черниговская Т. Есть ли место человеку в будущем мире искусственного интеллекта [Электронный ресурс]. Режим доступа: http://json.tv/ict_video_watch/tatyana-chernigovskaya-spbgu-est-li-mesto-cheloveku-v-buduschem-mire-iskusstvennogo-intellekta-20180209120328.

Elena V. Schelkonogova

PhD in Law, Associate Professor of the Department of Criminal Law

Ural State Law University

(Russia, Yekaterinburg)

Shelkonogova-ele@mail.ru

CRIMINAL LAW ON-LINE: THEORY AND PRACTICE OF DIGITALIZATION

Abstract: The relevance of the research topic is due to the active entry into the daily life of a person of digital and computer technologies. One of the spheres of life, in which computerization is actively gaining momentum is jurisprudence. It is enough to mention the existence of various reference and legal bases of legal acts, equipped with the ability to search by various parameters.

Despite the fact that the topic of digitalization is actively developed in the legal literature, the article has a novelty, because reveals various areas in which the use of computer programs containing algorithms, i.e. sequence of specific actions. It also addresses the issue of compliance with the principle of fairness when making decisions that are legally important by a computer or a qualified lawyer. In addition to the above, the problem of the digitalization of jurisprudence is considered both from the point of view of the fact that computer action algorithms can help a lawyer in his work, and from the position that law, in particular criminal law, is called upon to protect the sphere of computer activity.

Keywords: artificial intelligence, algorithm qualifications, the principle of justice, computer crime.

Цахуев Альберт Вагабович

эксперт отдела криминалистики следственного управления
Следственного комитета России по Республике Дагестан (г. Махачкала)
Albert05ck@mail.ru

СОБИРАНИЕ ЭЛЕКТРОННЫХ ДОКАЗАТЕЛЬСТВ ПРИ РАССЛЕДОВАНИИ УЧАСТИЯ ГРАЖДАН РОССИИ В НЕЗАКОННЫХ ВООРУЖЕННЫХ ФОРМИРОВАНИЯХ НА ТЕРРИТОРИИ ИНОСТРАННОГО ГОСУДАРСТВА

Аннотация: В статье рассматриваются электронные доказательства, получаемые при расследовании участия граждан Российской Федерации в незаконных вооруженных формированиях на территории иностранного государства. Автором рассматриваются особенности собирания электронных доказательств, использования устройств извлечения судебной информации из электронных устройств, фиксации электронных следов в протоколах следственных действий.

Ключевые слова: незаконные вооруженные формирования, электронные доказательства, собирание электронных доказательств, устройства извлечения судебной информации из электронных устройств, электронные следы.

На современном этапе развития Российской Федерации наибольшую угрозу национальной безопасности страны представляют преступления террористической направленности, приобретающие все более разнообразные формы и угрожающие масштабы.

По данным Главного информационно-аналитического центра (ГИАЦ) МВД России в 2014 году на территории Российской Федерации зарегистрировано 1 128 преступлений террористической направленности (АППГ +70,5%), в 2015 году – 1 538 (АППГ +35,8%), в 2016 году – 2 227 (АППГ +44,8%), в 2017 году – 1 871 (АППГ –16,0%), а за 2018 год – 1 679 (АППГ –10,3%)¹.

Наибольшую угрозу среди преступлений террористической направленности представляет участие граждан России в незаконных вооруженных формированиях на территории иностранного государства. В качестве наглядного примера участия российских граждан в незаконных вооруженных формированиях на территории иностранного государства приведем военный конфликт в Сирийской Арабской Республике, на территории которой в настоящее время действуют многочисленные НВФ, такие как «Джейш аль-Ислам», «Сабрий Джамаат», «Исламское государство», Хайят Тахрир аш-Шам и др., признанные террористическими и деятельность которых запрещена Решением Верховного Суда Российской Федерации на территории нашей страны².

По предварительным данным Генерального штаба ГРУ, ФСБ и других специальных служб России, в Сирийской Арабской Республике на стороне боевиков незаконных вооруженных формирований сражается около четырех тысяч выходцев из России³.

Выезд граждан России в Сирийскую Арабскую Республику и их участие в составе незаконных вооруженных формирований давно приобрела серьезный масштаб.

¹ Состояние преступности в Российской Федерации за 2015-2018 гг. // Официальный интернет-сайт МВД России [Электронный ресурс]. Режим доступа: <https://мвд.рф/reports> (дата обращения: 15.04.2019).

² Решение Верховного Суда Российской Федерации от 29.12.2014 по делу № АКПИ 14-1424С. Режим доступа: <http://nac.gov.ru/zakonodatelstvo/sudebnye-resheniya/reshenie-verhovnogo-suda-rf-t-29-dekabrya.html> (дата обращения: 25.04.2019).

³ Путин: в Сирии на стороне боевиков сражаются до четырех тысяч выходцев из РФ // ТАСС [Электронный ресурс]. Режим доступа: <http://tass.ru/politika/4047882> (дата обращения: 22.04.2019).

Многочисленные факты выездов граждан нашей страны и их участие в вооруженном конфликте на территории в Сирийской Арабской Республики в составе незаконных вооруженных формирований не остаются без внимания правоохранительных органов, возбуждаются многочисленные уголовные дела¹.

При совершении рассматриваемого преступления преступники используют современные технологии, среди которых наибольшей популярностью пользуется сеть Интернет, посредством которой через различные социальные сети и мессенджеры осуществляется передача огромного массива информации (листки о необходимости ведения военных действий против «неверных», о вступлении в ряды незаконных вооруженных формирований, о желании покинуть территорию России с целью последующего вступления в незаконные вооруженные формирования на территории иностранного государства и др.). Вся указанная информация образует комплекс фиксированных электронных следов и относится к категории электронных доказательств.

Законодатель не дает точного определения понятию «электронные доказательства», но следует отметить, что они являются одной из разновидностей вещественных доказательств и иных документов. Особенность электронных доказательств заключается в специфике их хранения, как правило, на жестких дисках, флэш-накопителях, серверах и др. В отличие от обычных предметов и веществ материального мира компьютерная информация не может существовать без электронных носителей информации².

По расследуемым уголовным делам и проводимым доследственным проверкам изымается большое количество разнообразных электронных устройств (например, компьютеры, ноутбуки, мобильные телефоны, планшетные компьютеры, видеорегистраторы и т.д.), содержащих в своей памяти различные виды электронных следов: контакты, сведения об устройстве, о соединениях между абонентами (исходящие, входящие, пропущенные звонки), переписка в виде SMS-сообщений, сообщений в социальных сетях и мессенджерах, фотоизображения, видео и аудиофайлы, геопозиционная информация, журнал использования интернет-браузеров, сведения о владельце устройства (пароли, логины, имена) и др. Указанные следы могут являться единственным доказательством по делу, в связи с чем, возрастает их криминалистическая значимость.

Как показывает практика, при расследовании уголовных дел рассматриваемой категории у следственных органов возникают сложности при работе с электронными доказательствами. Из положений действующего законодательства следует, что извлечение данных из мобильных устройств возможно при производстве следственных действий (осмотр предметов, обыск, выемка и др.), судебных экспертиз (компьютерно-технических) либо в ходе оперативно-розыскных мероприятий (исследование предметов и документов)³.

Изучение следственной и судебной практики расследования уголовных дел указанной категории показывает, что извлечение данных из мобильных устройств в ходе осмотра предметов занимает значительную долю и составляет 92% от общего количества извлечений, при производстве судебной компьютерно-технической экспертизы – 6,5%, в ходе оперативно-розыскных мероприятий – 1,5%.

Мы считаем, что осмотр предметов, в рамках которого производится собирание электронных доказательств, является наиболее оптимальным в связи с тем, что возникают обстоятельства, когда такое извлечение, в оперативно-тактическом смысле, необходимо произвести в кратчайшие сроки, а загруженность экспертов-компьютерщиков, зачастую,

¹ Цахуев А. В., Юсупкадиева С. Н. Участие граждан Российской Федерации в незаконных вооруженных формированиях на территории иностранного государства в целях, противоречащим интересам Российской Федерации // Евразийский юридический журнал. 2017. № 5 (108). С. 295.

² Вехов В. Б. Основы криминалистического учения об исследовании и использовании компьютерной информации и средств ее обработки: моногр. Волгоград: ВА МВД России, 2008. С. 83.

³ Зуев С. В. Электронное копирование информации – регламентация в УПК// Законность. 2013. № 8. С. 22.

затягивает сроки проведения компьютерно-технической экспертизы до нескольких месяцев.

И если раньше имелись сложности в связи с отсутствием отдельной нормы, то после последних изменений в Уголовно-процессуальный кодекс введена статья 164.1, которая регламентирует особенности изъятия электронных носителей информации и копирования с них информации при производстве следственных действий. Часть вторая данной статьи прямо указывает, что электронные носители информации должны изыматься в ходе производства следственных действий с участием специалиста¹.

При наличии непосредственно устройства, из которого необходимо извлечь электронные доказательства, каких-либо особых сложностей не возникает. Наибольшая сложность возникает, когда необходимо обнаружить, зафиксировать и изъять информацию, хранящуюся на значительном расстоянии от места производства предварительного расследования. Это касается случаев, когда сервер расположен на территории иностранного государства. Так, по делам рассматриваемой категории имелись факты необходимости изъятия информации, серверы которых располагались на территории Нидерландов, Дании, Швеции и других государств.

По сравнению с другими видами доказательств особенность обнаружения, фиксации, изъятия и последующего осмотра или назначения судебной экспертизы по электронным доказательствам заключается в том, что такие доказательства легко подвергаются необратимым изменениям и удалению, в связи с чем, при собирании любых электронных доказательств в ходе следственных и процессуальных действий необходимо соблюдать следующие тактические особенности:

- а) оперативность при собирании электронных доказательств;
- б) обязательное привлечение соответствующих специалистов, как правило, имеющих знания в области компьютерной техники;
- в) применение современных аппаратно-программных комплексов извлечения информации из электронных устройств.

Безусловно, полноценная работа с электронными устройствами возможна только при хорошей оснащенности правоохранительных органов современной высокотехнологичной криминалистической техникой, позволяющей извлекать полную (включая удаленную) информацию из памяти мобильных устройств, а также различного рода накопителей данных (карт памяти, SIM-карт и др.). К такой технике относятся аппаратно-программные комплексы «UFED», разработанный израильской компанией «Cellebrite», «XRY» (разработчик – шведская компания «Micro Systemation»), программный комплекс «Мобильный криминалист» (разработчик – российская компания «Oxygen Software») и др.²

Использование электронных доказательств является перспективным направлением раскрытия и расследования уголовных дел рассматриваемой категории. В последнее время особенно стало актуальным использование сведений из различных социальных сетей и мессенджеров (например, WhatsApp, Viber, Telegram, ВКонтакте, Одноклассники.ru и др.), а также различных видео-хостингов.

Хочется отметить, что успех расследования уголовных дел указанной категории во многих случаях зависит от соблюдения следователями и другими сотрудниками правоохранительных органов требований, предъявляемых к фиксации, изъятию, упаковке и осмотру любых электронных носителей информации.

Результаты проведенного анкетирования следователей, в производстве которых находились уголовные дела рассматриваемой категории, свидетельствует о сложившемся

¹ Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ (ред. от 01.04.2019, с изм. от 17.04.2019) (с изм. и доп., вступ. в силу с 12.04.2019) // СПС «КонсультантПлюс» [Электронный ресурс]. (дата обращения: 05.05.2019).

² Хмелева А. В. Тактические особенности назначения судебных экспертиз // Эксперт-криминалист. 2014. № 4. С. 12.

у них мнению в части нарушения конституционных прав владельцев мобильных устройств, из которых осуществляется извлечение данных, однако, оно является неверным, так как в Определении Конституционного суда Российской Федерации от 25.01.2018 № 189-О сказано, что «Проведение осмотра и экспертизы с целью получения имеющей значение для уголовного дела информации, находящейся в электронной памяти абонентских устройств, изъятых при производстве следственных действий в установленном законом порядке, не предполагает вынесения об этом специального судебного решения, и они не могут расцениваться как нарушающие его конституционные права».¹

В ходе производства следственного действия возможно осуществление копирования информации, содержащейся на электронном носителе информации. В протоколе следственного действия необходимо указать все примененные технико-криминалистические средства, начиная со средств фото либо видеофиксации, заканчивая сложными аппаратно-программными комплексами извлечения информации из электронных устройств, а также результаты их применения. К протоколу следственного действия необходимо прилагать электронные носители с информацией (флэш-накопители, оптические диски, внешние жесткие диски и др.), извлеченной из других электронных носителей информации в ходе производства следственных действий.

В современном уголовно-процессуальном законодательстве изложенные нами положения как уже было отмечено реализуются посредством производства следственных действий, назначения судебных экспертиз и др. Однако, особенность совершения рассматриваемых преступлений, специфика следообразования и другие факторы негативно сказываются на эффективной борьбе с данными преступлениями.

Мы считаем, что выходом из сложившейся ситуации является обобщение имеющихся знаний по указанной проблеме с учетом мнений научных и практических сотрудников, создание единой методики с целью решения различных проблем, возникающих при работе с электронными доказательствами, а также введение в Уголовно-процессуальный кодекс статьи, регламентирующей порядок производства осмотра электронных устройств (компьютеров, мобильных устройств, флэш-карт и др.).

Список литературы

1. Вехов В. Б. Основы криминалистического учения об исследовании и использовании компьютерной информации и средств ее обработки: моногр. Волгоград: ВА МВД России, 2008. 404 с.
2. Зуев С. В. Электронное копирование информации – регламентация в УПК// Законность. 2013. № 8. С. 22–23.
3. Состояние преступности в Российской Федерации за 2015-2018 гг. // Официальный интернет-сайт МВД России [Электронный ресурс]. Режим доступа: <https://мвд.рф/reports>.
4. Хмелева А. В. Тактические особенности назначения судебных экспертиз // Эксперт-криминалист. 2014. № 4. С. 12-15.
5. Цахуев А. В., Юсупкадиева С. Н. Участие граждан Российской Федерации в незаконных вооруженных формированиях на территории иностранного государства в целях, противоречащим интересам Российской Федерации // Евразийский юридический журнал. 2017. № 5 (108). С. 294-296.

¹ Определение Конституционного суда Российской Федерации от 25.01.2018 № 189-О «Об отказе в принятии к рассмотрению жалобы гражданина Прозоровского Дмитрия Александровича на нарушение его конституционных прав статьями 176, 177 и 195 Уголовно-процессуального кодекса Российской Федерации» // СПС «КонсультантПлюс» [Электронный ресурс]. Режим доступа: <http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=ARB002&n=527893#06295194616962025> (дата обращения: 25.04.2019).

Albert V. Tsakhuev

Expert of Forensic Department of the Investigations Directorates
of the Russian Federation Investigative Committee for the Dagestan Republic (Russia,
Makhachkala)
Albert05ck@mail.ru

**GATHERING ELECTRONIC EVIDENCE IN THE INVESTIGATION OF THE
PARTICIPATION OF CITIZENS OF THE RUSSIAN FEDERATION IN ILLEGAL
ARMED FORMATIONS ON THE TERRITORY OF A FOREIGN STATE**

Abstract. The article deals with the electronic evidence obtained in the investigation of the participation of citizens of the Russian Federation in illegal armed formations on the territory of a foreign state. The author considers the features of the collection of electronic evidence, the use of devices for extracting judicial information from electronic devices, the fixation of electronic traces in the protocols of investigative actions.

Key words: illegal armed groups, electronic evidence, collection of electronic evidence, devices for extracting judicial information from electronic devices, electronic traces.

Научное издание

ТЕХНОЛОГИИ XXI ВЕКА В ЮРИСПРУДЕНЦИИ

Материалы
Всероссийской научно-практической конференции

(г. Екатеринбург, 24 мая 2019 года)

Компьютерная вёрстка: Д. В. Бахтеев

Дизайн обложки: К. О. Хрущёва

Уральский государственный юридический университет
620137, г. Екатеринбург, ул. Комсомольская, 21

Кафедра криминалистики УрГЮУ
620137, г. Екатеринбург, ул. Комсомольская, 21
Тел.: +7 (343) 367-40-95

Подписано в печать 22.05.2019. Формат. 60*84/16
Бумага офсетная.
Тираж 80 экз.

Отпечатано с готового оригинал-макета в типографии
ООО «Издательство УМЦ УПИ»
г. Екатеринбург, ул. Гагарина, 35а, оф. 2.